Emergency Notification on Mobile Devices –

A Trade-off between Protection Motivation, Privacy Concern and Personalised Notification

---

A thesis submitted in partial fulfilment of the requirements for the Degree of Master of Commerce in Information System

by Jing Zhang

University of Canterbury

2017

Table of Contents

List of Table and Figure

Acknowledgments

I would first like to thank my supervisor Assoc. Prof. Annette Mills. I still remember you were busy working out my enrolment when we first met. It was a great relief to the tension. Thanks for your help throughout the 18-month masters programme. Thanks for your endless patience in helping me to refine my research project. You lent me a hand both on my postgraduate study and in my life in New Zealand. Many thanks.

I would also like to thank my co-supervisor Nelly Todorova. Thank you so much for all your enthusiasm, guidance and unrelenting support throughout this process. Thanks for your thoughtful insights in our research and thanks for your clear and detailed instructions when I was unclear. Thank you so much.

I would also like to express my gratitude to the three faculty in INFO614 i.e. Prof. Markus J. Milne, Assoc. Prof. Beverley Lord and Dr. Stephen Wingreen. I am thankful to you for your time and effort in making INFO 614 an interesting and helpful paper. And thanks to all the other faculty in the College of Business and Law for providing me with all the necessary facilities for the research.

I am also grateful to Prof. Dr. Christian M. Ringle of the Northern Institute of Technology (NIT), who dedicated an amazing course on PLS and to Dr. Carol Saunders, an outstanding research professor from Northern Arizona University. Thanks to their generosity in sharing their wisdom and insights in my research area.

I would also like to thank my dear classmates and friends who were involved in the survey pre-test of this research project. Without their passionate participation and input the formal survey would not have been successfully conducted. I also place on record, my sense of gratitude to one and all who directly or indirectly have lent their helping hand in this venture.

Finally, I must also express my very profound gratitude towards my parents in China and towards my husband for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without them. Thank you.

Abstract

The world today is increasingly being impacted by natural disasters and other threats with both human and natural causes. The number of natural disasters worldwide has increased by more than four times in the last few decades (Gutierrez, 2008). Their effect is also concerning with the average economic impact increasing more than tenfold over the last few decades from US$14 billion in 1976-1985 to US$140 billion in 2005-2014, and the number of persons affected rising from 60 million to over 170 million for the same periods (GFDRR, 2016). This highlights the significant role of contemporary emergency management in order to minimize the potential damage and impact on human lives. A Personalised Mobile Emergency Alert Service (PMEAS) is one of the endeavours that have been adopted by many developed countries. It provides prompt emergency alerts via mobile devices based on user's current location and personal profile. PMEAS has succeeded in saving lives and properties in many cases (http://www.nws.noaa.gov).

However, similar to the other personalised online services that require users to register or disclose personal information in exchange for a service that is tailored to their needs, the users of PMEAS are also expected to disclose personal information to receive customized notifications. Thus, users would be exposed to the potential risks that raise privacy concerns. This study examines the factors that influence an individual to disclose personal information in order to use PMEAS. Since user's information disclosure is vital for a PMEAS to be successful, the results of this study would also facilitate the understanding of the motivators and inhibitors of information disclosure in PMEAS.

This paper reports on an empirical study that investigates individual's willingness to disclose personal information in order to use PMEAS, focusing on mobile users in New Zealand. Protection Motivation Theory (PMT) is used as a theoretical framework supported by the trade-off between personalisation and privacy concern. The results suggest that applying PMT is useful for explaining an individual's willingness to disclose personal information to use a PMEAS. By improving the understanding of users' expectations and concerns, the research outcomes provide insights to the government agencies and PMEAS providers to design and implement better services and to perform better risk management.

1. Introduction

The twenty-first century has been dubbed the "century of disasters". The total cost of disasters worldwide in 2010 was 100 billion US dollars, which was roughly the same amount given by OECD countries as development aid to developing nations in the same period (OECD, 2012). The mortality and economic loss associated with extensive disaster risks (i.e. minor but recurrent disaster risks such as flash floods, landslides, storms and fires) are trending up. Extensive disasters have resulted in a total loss of 94 billion US dollars in 85 countries and territories in the last decade (GAR, 2015). All countries are directly or indirectly affected by disasters caused by climate change, demographic changes and social dynamics, leading to significant challenges for the governments of cities, regions, states, and countries. Being able to notify people in the case of disasters is important for saving lives and properties, as well as to mitigate other potential damages.

Disasters such as earthquakes provide few warning signs and can causes massive damages. Both the 2010 Haiti earthquake and the 2011 Great East Japan earthquake and Tsunami led to irretrievable loss for the people and the countries. More than 15,000 deaths were reported in Japan's earthquake and more than 230,000 deaths were confirmed by the Haitian government. The Haitian earthquake resulted in $7.8 billion to $8.5 billion in damages while the physical damage for Japan has been estimated to be from $195 billion to $305 billion. (CRS Report for Congress, 2011; Haiti Earthquake: Facts, 2015). The primary cause for such huge damage was that people were unprepared when the earthquakes struck. In other words, there was no warning, and correspondingly no earthquake preparedness action could be taken before the earthquake. When the intense shaking happened, people were only able to take limited self-protective actions since some damages such as power cuts and falling objects were caused within a few seconds. This made it even harder for people's evacuation (Stuff, 2010).

Traditional emergency alert approaches such as sirens, radio, television, and landlines can only reach a limited number of people. For disasters that require immediate protective actions, these approaches may miss potential victims who do not have immediate access to those media. In the meantime, as the mobile connection rate is incredibly high and continuously growing (e.g. the number of mobile phones in use is

exceeding the population in many countries such as China, New Zealand, etc. (www.statista.com), using mobiles for emergency notification purposes becomes an ideal option for most countries for their emergency management.

1.1 Personalised Mobile Emergency Alert Service (PMEAS)

In response to the growing rate of acute shocks (such as flash floods, bush fires, earthquakes, tsunamis, pandemics and terrorist attacks), which are extremely time-sensitive in terms of relief efforts, many countries have been enhancing their emergency management systems using Information and Communication Technology (ICT) in recent years.

As part of these endeavours, emergency notification via mobile devices has been introduced by many developed countries as an effective method of issuing early warnings, including the USA, the UK, Australia and Japan. As a complement to traditional alert avenues such as the radio, television and sirens, mobile alerts can automatically “pop up” on a mobile device screen, giving clear notice of what type of emergency is in progress, when and where it happened or will happen, as well as what action the receiver should take to mitigate threats.

1.1.1 Definition of PMEAS

A Personalised Mobile Emergency Alert Service (PMEAS) is a public safety service system that provides emergency alerts before or during an emergency to mobile devices. This service is used by governments and authorized communication technology companies around the world. It enables people to take actions when they receive alerts.

Mobile Emergency Alerts are text-like messages that are sent to users' mobile devices in case of emergency. The types of emergency alerts include but are not limited to severe weather information, natural hazards, imminent threats, and national security and local incident information. The alerts typically include the emergency type and duration, any action you should take and the emergency service provider issuing the alert. For example: "Flood warning for lower Christchurch till 1:00PM. Prepare. Avoid Travel. Check media. Canterbury Civil Defence."

To receive the alerts, individuals would sign up to the service through a mobile device which enables the service provider to tailor the alert messages and recommended actions to the user based on their location (e.g. registered location and current location) and other relevant personal information such as gender, age and health information, if disclosed.

1.1.2 The Use of PMEAS

In the USA, "Wireless Emergency Alerts" (WEA) is a public safety system that allows customers who own certain types of wireless phones and other enabled mobile devices to receive geographically targeted, text-like messages alerting them of imminent threats to safety in their area" (www.fcc.gov). For example, a tornado warning from the National Weather Service triggered a WEA which saved as many as 34 lives in East Windsor, Connecticut. In another incident in New York, a tornado with 100 mph speed destroyed about 20 homes. However, no significant injuries were reported because most of the residents followed the emergency notifications that were relayed on their phones and took shelter in their basements immediately upon receiving the alert message. In Japan, the Earthquake Early Warning System (EEWS) is regarded as one of the most advanced disaster warning systems in the world: "It provides advance announcement of the estimated seismic intensities and expected arrival time of principal motion" (www.jma.go.jp).

Some systems include an opt-out mechanism, which initially provides information notification without the users' consent. The users can then choose to 'opt-out' of receiving notifications. However, alerts for most systems are only issued to users who have registered or subscribed to the service. For instance, the government of Hillsborough County in Florida (HCFL) implemented an "HCFL alert", which is a notification system that is designed to provide subscribers with critical emergency information and other important informational messages. The system enables subscribers to customise their profile to receive voice, text or e-mail messages. People who have signed up to receive the messages are asked to register online by creating a profile, and provide contact details (such as their e-mail address, and mobile, home and work phone numbers) and address information, which can be verified. This enables personalised emergency alerts based on the receiver's registered location. However, the

drawback of this service is that the subscriber may be in a different location that is not registered, so does not receive the alerts that are relevant to their current location.

Mobile Alert Systems in Australia have mitigated this issue by enabling emergency notifications to be issued to the receiver's current location. According to the Australian Mobile Telecommunication Association, "The location-based enhancement to Emergency Alert allows emergency warnings to be sent to mobile telephones based on the physical location of the mobile handset at the time of an emergency, including residents and people travelling through a threatened area." (www.amta.org.au). Another Australian organization called Early Warning Network (EWA), provides live severe weather warning across Australia to those who use EWA apps on their mobile devices and allows real-time GPS tracking. In one of the latest warning message issued on 31 March 2017 at 6:12 pm was about potential severe thunderstorms that were going to happen in half an hour. Recommended protective actions were provided in the warning message to advise people to "secure loose outside objects", "avoid remaining in the open when storms threaten" and "avoid driving into water or unknown depth and current" (www.ewn.com.au).

Mobile alert systems are extremely important because many countries like USA, Australia and elsewhere frequently experience a wide range of natural disasters including fires, floods, tornados, severe storms, earthquakes and landslides. However, as a prerequisite, the potential receiver must be willing to disclose their mobile device location data and other personal information to the notification provider. In other words, the more personalised the notification that the user would like to receive, the more personal information (such as location, demographics, status of health) the individual is required to disclose. This leads to the issue that people may not be willing to disclose their personal information, and to give up some of their privacy in exchange for customized services (Kim and Lee, 2009). When personal information is required by an online service, concerns are usually raised about the potential misuse of the information (Zhao, 2012). This argument is supported by a prior study (Xu et al., 2009) that revealed users of location-based services are reluctant to disclose personal information when they believe there is a high potential of privacy invasion or a lack of effective protection of their personal information. General privacy concern, as "an individual's general tendency to worry about information privacy" (Malhotra et al., 2004), is believed to play a vital role in influencing an online user's privacy perceptions and behaviours when interacting with online services (Li et al., 2011). Therefore,

understanding how an individual's privacy concern would influence his or her intention to disclose information to a PMEAS is important to both PMEAS providers and the success and growth of other location-based services.

1.2 Research Focus and Questions

In today's world, the threat of disasters and other emergencies is increasing. It is therefore expected that increasing emphasis will be placed on the use of Personalised Mobile Alert Service (PMEAS) worldwide. Since most systems to-date are opt-in systems[1], understanding an individual's willingness to sign up into a PMEAS is particularly important for system success.

Research shows individuals have different general tendencies towards being risk averse or risk taking (Wildavsky and Dake, 1990). Furthermore, perceptions of a particular threat vary across individuals. This may partly explain differences in acceptance of PMEAS because people are not equally worried about the same threat. Some may perceive the risks of a particular threat as great while others think of it as small (Wildavsky and Dake, 1990).

A number of studies have examined the impact of perceptions of threat on behavioral intention (Floyd et al., 2000; Leventhal, 1970; Rogers, 1975; Rogers, 1983; Witte and Allen, 2000). One model that has been widely used to examine "threats" is **Protection Motivation Theory (PMT)** introduced by Rogers (1975), which embodies the idea of "fear appeal" (i.e. the contents of a communication describing the unfavourable consequences that may result from failure to adopt the communicator's recommendations). PMT is a widely used conceptual model that seeks to understand how "fear appeal" may influence an individual's risk perceptions, and in turn their response behavior (Salleh et al., 2013). PMT has been widely used in research on health-related issues (Fry and Prentice-Dunn, 2006; Prentice-Dunn et al., 2009; Salleh et al., 2013), which investigate the cognitive processes that occur when individuals receive health information that highlights certain health-related risk situations that may impact their well-being (Fry and Prentice-Dunn, 2006). In the same vein, an alert notification from PMEAS (whether it is a severe hazard alert or a general notification

[1] People have to actively sign up to a service provider to use the mobile emergency alert service.

about road works or accidents) may range from being an informative communication, to representing a "fear appeal" about a threat that can bring harm to an individual's well-being, (Milne et al., 2000). Hence, both health-related information and emergency notifications share similar characteristics of a threat, which may in turn motivate people to take actions to protect themselves from a risky situation, based on their perceptions of the risk of the threat (Salleh et al., 2013).

Like health-related information, a PMEAS can only be successful if, in the case of an emergency, people are willing first to receive the notification, and then to act on the notification to mitigate the threat and protect themselves. As a first step, it is essential therefore to understand individuals' perceptions of the threat (e.g. their perception of the severity of the threat and their susceptibility to the threat), their potential fear of the threat, and their intention to protect themselves by receiving messages about the threat that are conveyed by the PMEAS providers (Boer and Seydel, 1996). Previous studies further indicate that the stronger the individual's protection motivation, the more effective the emergency communication is expected to be (Mulilis and Lippa, 1990).

On the other hand, despite the significant opportunities offered by personalised mobile emergency alert services, they also raise concerns about individuals' privacy which may be a key inhibitor of their use (Li et al., 2011; Xu et al., 2009). From the users' perspective, they may identify high value in receiving prompt emergency alerts that help them to make the right decisions in responding to a risk or threat. At the same time, they may also have concerns about disclosing personal information and being monitored by the notification providers and other receivers of their information. The result is that users are faced with a dilemma over whether to give up their privacy (in terms of how much and what kind of information they disclose) in exchange for the potential value of a personalised emergency alert service.

The research objective of our study is to examine individual's willingness to disclose personal information in the context of using a PMEAS. Given the broad nature of the research objective, the main research focus is placed on an individual's protection motivation regarding an emergency in relation to their *intention to disclose personal information in exchange for emergency notifications that are tailored to their current situation*. In addressing the research question, this study will also examine the impact of the trade-off between privacy concern and personalisation on an individual's intention to share personal information when using a PMEAS.

The specific research questions are:

(1) What factors impact an individual's willingness to disclose personal information in the context of using a PMEAS?
(2) What impact does the trade-off between privacy concern and personalisation have on an individual's willingness to disclose personal information in the context of using a PMEAS?
(3) What impact does risk perception have on an individual's willingness to disclose personal information in the context of using a PMEAS?

To answer the above questions, this study applies the full nomological model using all potential PMT constructs, which is integrated with privacy concern and personalisation to contextualize the theoretical framework. The results of the empirical study are expected to extend the current application of the PMT into emergency management. It is also expected to contribute to the knowledge of Personalised Mobile Alert Services (PMEAS) both theoretically and empirically.

This study reports on the findings from a survey of mobile users in New Zealand. New Zealand, as a country is frequently threatened by natural disasters (such as earthquakes, flash flooding and so on) due to its geographical position and climate type. To mitigate these disasters, there are PMEAS available that provide personalised emergency alerts to people who have subscribed or registered for the services (such as Hazards[2] and LERT Info). Most of the existing PMEAS in New Zealand and elsewhere (e.g. Australia, USA) allow a personalised notification service based on a user's profile and current location. Hence, it is only by disclosing adequate personal information to the service provider (e.g. allowing the service to monitor the user's current location, or sharing health status or disability information) can the effectiveness of these PMEAS be ensured in the case of an emergency. Nevertheless, it is reported that not many people are using these services. For example, around 35,000 people are subscribed to the Auckland local emergency notification app, which is only approximately 2.4% of the local population (Auckland Council, 2016). It is therefore important to understand people's perceptions of PMEAS. In New Zealand, this is important as the country is under threat from potential emergencies, and has in fact, been impacted by a number of

[2] "Civil Defence Auckland" (used to be running by Auckland local government) has been extended to nationwide level service "Hazards" in June, 2016, which enables monitoring of both pre-indicated and current positions across New Zealand.

natural disasters in the past few years (e.g. earthquakes and flooding). Potential users are therefore expected to be benefit from using PMEAS in this context.

1.3 Thesis Structure

This thesis is divided into seven chapters. It is structured as follows.

Chapter 1: Introduction
The first chapter presents an overview of the research topic by introducing the background of the PMEAS. It highlights the importance of understanding the factors that influence individuals to use a PMEAS in today's world by addressing the research gap, defining the research scope and research questions, and pointing out potential research contribution.

Chapter 2: Literature Review
This chapter reviews the literature on key topic areas related to this study. First, it highlights the key research challenges in Emergency Alert, ICT and Mobile Notification. Then, literature on Fear Appeal Theory, Protection Motivation Theory, and the Privacy/Personalisation trade-off are discussed. Finally, the research gaps are addressed based on prior literature.

Chapter 3: Model Development
This chapter outlines the key aspects of PMT and related constructs. The conceptual model is then proposed and the hypotheses are discussed.

Chapter 4: Research Methodology
Chapter 4 describes how this research was structured and conducted in relation to the positivist approach and quantitative methods used as well as instrument development. The administration of the questionnaire and the procedure of data collection are explained. It is followed by the discussion of instrument development.

Chapter 5: Data Analysis
This chapter presents the data analysis and results of model testing. It begins with the demographics of the valid responses. Then, the result of the manipulation checks for

fear-appeal is presented. This is followed by the evaluation of outer (measurement) model and the inner (structural) model.

Chapter 6: Discussion

In this chapter, the research findings are discussed in relation to the research questions that guide this study and the prior research.

Chapter 7: Conclusion

The final chapter highlights the research contribution, followed by the implications for practice. The limitations and directions for future work are also addressed in this chapter.

2. Literature Review

2.1 Emergency Alert, ICT[3] and Location-based Mobile Notification

An "emergency" is defined as "a serious, unexpected, and often dangerous situation requiring immediate action." (Oxford Dictionary). It is usually defined in a certain time and space, with a threshold value (e.g. mortality rate) to be recognized. An emergency relates best to response, and usually calls for rules of actions and an exit strategy (WHO, 2016).

In the US, Personalised Mobile Emergency Alert Service (PMEAS) have been implemented for both national and local services. These location-based emergency alert services provide the government and authorized organization the capability to provide immediate communications and information to the general public at the national, state and local area levels during periods of national emergency. It also provides national and local governments, as well as the National Weather Service with the capability to provide immediate location-specific communications and information to the general public concerning emergency situations posing a threat to life and property (Federal Information and News Dispatch, 2015).

Previous literature in emergency alert systems largely focus on the design and delivery of effective notification services. For example, the study done by Palen et al. (2010) presents a vision of the future emergency management system by incorporating information from members of the public during the mass emergency events. Most of the research in this area was conducted from a designer's perspective rather than a user's perspective. A few empirical studies have been done to identify factors that influence people's intentions to use emergency alert systems. Using theoretical frameworks such as the Technology Acceptance Model (TAM) and Unified Theory of Acceptance and Use of Technology (UTAUT) (Choy et al., 2016; Haataja et al., 2011; Wu et al., 2008), prior studies have identified factors such as trust, perceived benefits, perceived usefulness and perceived ease of use as having significant impacts on user's intention to adopt such services. For example, trust and perceived benefits were found

[3] **ICT**: Information and Communications Technology

to be significant in motivating students' intention to use emergency notification services in campus emergencies (Choy et al., 2016).

Other research on location-based services also suggests that using location-based emergency alert service raises issues related to trust, risk perceptions, and privacy concern for users. (Aloudat and Michael, 2011). Current studies in emergency alerts and information disclosure have focused on user's privacy concerns, trust and behavior intention when using location-based emergency alert services (Aloudat and Michael, 2011; Yang et al., 2003; Zeithaml et al., 2000). For example, users may worry about whether the information collected for emergencies will be used for other purposes without their consent (Smith et al., 1996). In an Australian-based study of location-based emergency service, Aloudat and Michael's (2011) conducted an open-ended survey among the general public, and interviews of key informants who were working closely with local PMEAS. The survey respondents were asked about their perceptions of privacy, while the key informants were asked to share their experience and insights about location-based emergency services. The research findings show that when using location-based emergency services, extensive location information and other identifying personal data are collected, which may induce the users' privacy concerns. Moreover, people tend to trust the information in alert messages if they regard the public authorities as reliable and trustworthy.

A number of factors need to be examined to gain a deeper understanding of individual's willingness to disclose personal information in using PMEAS. These include the nature of an emergency which may arouse individual's fear of a certain threat, the individual's risk perceptions of the threat, how they would like to respond to the potential damage and protect themselves from being hurt by the threat, and other factors such as fear and risk perceptions about the emergency. Prior research suggests that emergencies such as natural disasters present a complex and unpredictable situation with regards to the response actions (e.g. feel hopeless and do nothing, immediately seeking evacuation or other protective actions) (Ren et al., 2008). Psychologists (Fritz and Marks, 1954) also point out that people's emotional reactions to disasters can be very different and then determine their behaviour in disasters. Therefore, understanding individual's risk perception and how to motivate people to engage in protective responses becomes important. To address the important gaps in the existing literature, the following sections in Chapter 2 review the key theories that relate to this research - fear appeal theory, protection motivation theory and information privacy.

2.2 Fear Appeal Theory and Models

Fear is a "relational construct, aroused in response to a situation that is judged as dangerous and toward which protective action is taken." (Rogers, 1975). The situation itself, is usually described by a fear appeal, which is "an informative communication about a threat to an individual's well-being." (Milne et al., 2000). Other researchers also define fear appeals as "persuasive messages that attempt to arouse fear by emphasizing the potential danger and harm that will befall individuals if they do not adopt the messages' recommendation." (Tannenbaum et al., 2015). The core issue in fear-appeal studies is to establish and conceptualize the way a fear-arousing communication can influence individual's attitude, behavioral intention and actual behaviour (Milne et al., 2000). This is relevant to this study as an emergency notification can be viewed as a "fear arousing communication" that may impact a person's attitude and motivation towards taking actions to protect themselves (e.g. being willing to receive an emergency notification and advice on actions to take).

Beginning in the 1970s, fear appeal theories have spawned three main groups of theories: drive theories, parallel response models and subjective expected utility (SEU) models (Witte and Allen, 2000). Drive theories as the earliest stream in fear appeal research, indicate that the extent of fear triggered by fear appeal performs as a driver to motivate actions. The central argument of drive theories is that fear can either motivate or interfere with protective behaviour (Hovland et al., 1953; Janis, 1967; McGuire, 1969).

The Parallel response model was initially proposed by Leventhal (1970) in 1970s. His model suggests there are two dependent cognitive processes triggered by fear appeals: danger control process (e.g. adopting the suggested information) and fear control process (e.g. avoiding threatening information to relieve the fear emotion) (Leventhal, 1970). Although researchers criticize the model as untestable, the idea of separating the emotion of fear from the cognitive process offered great insight to later research (Witte and Allen, 2000).

Subjective expected utility (SEU) models such as Protection Motivation Theory (PMT) focus on explaining the relationship between fear appeal and behavioral change in a logical manner (Floyd et al., 2000; Rogers, 1975; Rogers, 1983; Witte and Allen, 2000). Using these models, the results of studies of the fear appeal communication states there

is a linear relationship between fear appeal and behavioral change (Witte and Allen, 2000). The more intensive the fear appeal, the stronger the behavioral intention in terms of engaging adaptive responses (Boer and Seydel, 1996). Researchers are in favor of using Protection Motivation Theory (PMT) for two main reasons. First, the effectiveness of fear appeal has been clarified in the protection motivation theory by accounting for two cognitive mediating processes, i.e., a threat appraisal process (as weighing perceived severity and vulnerability of the threat against mal-adaptive rewards) and a coping appraisal process (as weighing response efficacy and self-efficacy of taking the adaptive response against the response cost). The second reason is that protection motivation theory is the only fear-appeal theory that incorporates self-efficacy, which is believed to be one of the most significant components influencing the attitude and behavioral change (Floyd et al., 2000).

2.3 Protection Motivation Theory (PMT)

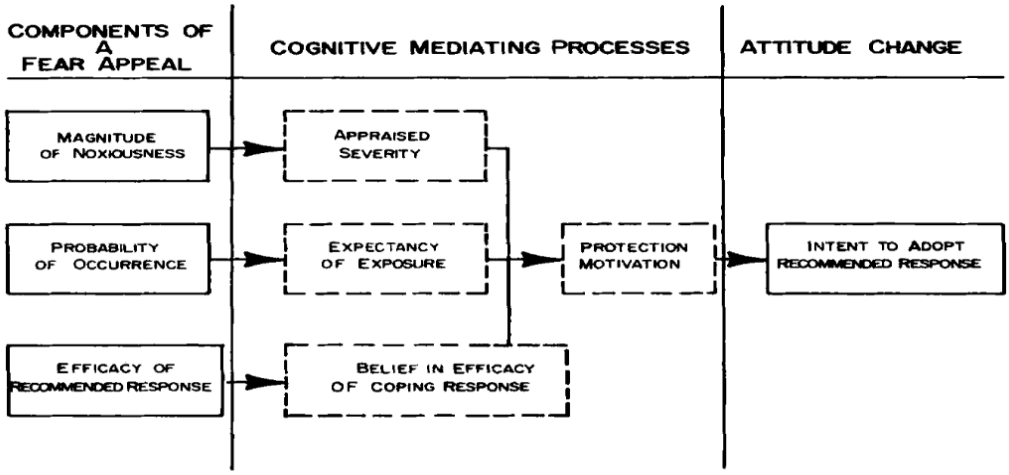
Protection Motivation Theory (PMT) was initially posed by Rogers (1975) to explain individual's attitude change and behavioral intention in response to a fear appeal, which examines individual's risk perceptions toward a threat in relation to their appraisal of their ability to cope with it. The theory has been widely accepted and applied in health-related behaviour research (Floyd et al., 2000; Milne et al., 2000; Prentice-Dunn and Rogers, 1986; Rippetoe and Rogers, 1987), as well as some IS-security research (Herath and Rao, 2009; Siponen et al., 2006; Vance et al., 2012). Prentice-Dunn et al. (2009) conducted a research that examined the usefulness of creating brief persuasive appeals to promote healthy sun-protective behavior. Fry and Prentice-Dunn (2006) conducted an experiment to test whether an educational intervention would promote breast self-examinations. The results showed that participants who received educational information performed higher rational problem solving and adaptive responses towards a breast cancer threat. Boss et al. (2015) contributed a longitudinal study of data backup to the literature using the full nomology of PMT constructs. The results showed that participants who perceived a greater fear appeal were more strongly motivated to carry out the corresponding protective behaviour (i.e. to do backups, correspondingly more actual backups took place.)

Figure 1 illustrates the schema of Protection Motivation Theory. The theory was originally developed within the framework of a fear-arousing communication. As such,

the communication starts from a fear appeal, which then generates a cognitive mediating process, and eventually leads to the potential change of attitude and behaviour. Protection Motivation Theory, therefore, provides a significant social cognitive account of individual's protective behaviour (Milne et al., 2000).

According to Rogers's (1975) Protection Motivation Theory, fear-evoking persuasive messages are composed of three crucial parts: (a) the magnitude of noxiousness (fear) of a depicted event; (b) the probability of that event's occurrence; and (c) the efficacy of a protective response. Protection Motivation is therefore positively associated with the three components in a persuasive message. That is, the greater the noxiousness (fear), probability and efficacy in the message, the greater the aroused protection motivation. In addition, according to Protection Motivation Theory, since each of the three key elements is essential to a persuasive message, if any of those elements is missing, the message will not trigger a protection motivation response (Milne et al., 2000). An individual's protection motivation, as the key concept of Protection Motivation Theory, therefore comprises the listener's evaluation of the noxiousness (fear), probability and efficacy of the persuasive message as well as their drive to take steps to avoid a potential threat based on their perception of the persuasive message (Milne et al., 2000).

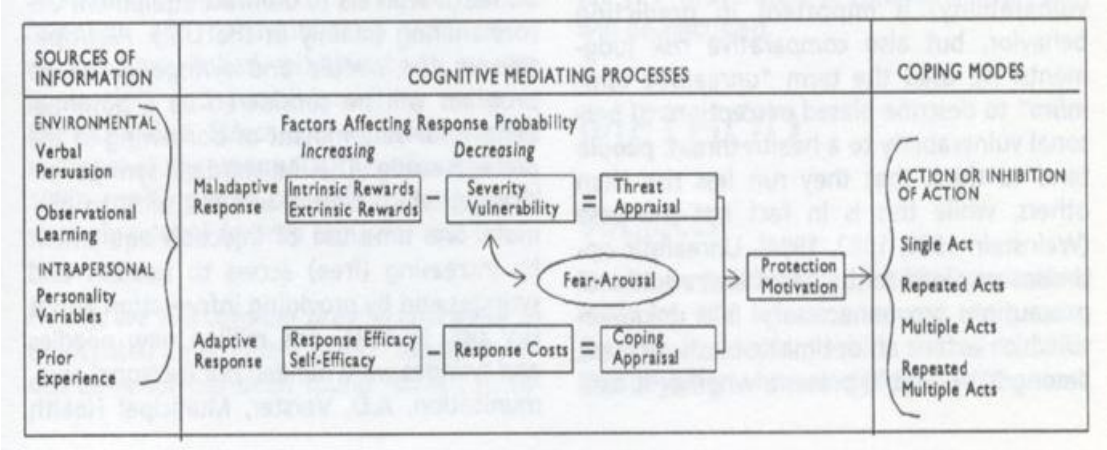
Figure 1: Schema of Protection Motivation Theory (Rogers, 1975, p99)



2.3.1 The PMT Model's Structure and Variables

The early version of the Protection Motivation Theory (PMT) (Figure 1) emphasized the three components of a fear appeal: magnitude of noxiousness, probability and the efficacy of recommended response, while the later version of the Protection Motivation Theory (Rogers, 1983) extended the model to a more general theory of persuasive communication (Conner and Norman, 2005). Maladaptive reward (perceived benefits of not performing the adaptive response to the threat event; Rogers, 1983.) was added as an additional coping response in the appraisal process, such as "Not using an anti-malware application saves me time." (Myyry, et al., 2009). The original coping appraisal was also expanded by incorporating self-efficacy into the model (Milne et al., 2000), as illustrated in Figure 2.

Figure 2: Revised Protection Motivation Theory (Rippetoe and Rogers, 1987, p597)



The revised PMT model, which is also referred to as the PMM, posits that people coming across an environmental threat stimulates a parallel (unordered) sequence of two cognitive appraisal processes (threat appraisal and coping appraisal), which then mediate the option for coping modes. In this context, a *threat* is defined as "something that is a source of danger that can bring harm (physical or mental) to an individual." (Junglas et al., 2008). As such, a threat appraisal measures the rewards of a maladaptive response against the severity and vulnerability of the threat. It is believed that perceived severity and vulnerability can predict more behavioral intention to engage protective behaviour while the reward of maladaptive response can predict less intention (Ruthig,

2016). For example, in the case of smoking, a maladaptive response may lead to both intrinsic rewards (e.g. physical and mental pleasure) and extrinsic rewards (e.g. peer approval). *Severity* refers to the perceived severity of the disease that is caused by smoking (Yan et al., 2014), whereas *vulnerability* is the possibility of the occurring of such a disease to the individual (Yan et al., 2014). Fear is also included as an important component in the threat appraisal. If the perceived severity and vulnerability are high, the threat appraisal leads to fear (Arthur and Quester, 2004). Fear indirectly enhances protection motivation by mediating the impact of perceived severity and vulnerability of the threat on protection motivation (Boer and Seydel, 1996).

Coping Appraisal evaluates the response efficacy and self-efficacy against response costs. Research has verified that response efficacy (belief in protective behaviour will be effective in protecting against threat) and self-efficacy (belief in individual's ability to perform the protective response) predict stronger intention, whereas response cost predicts less intention to engage the protective behaviour (Ruthig, 2016). In the case of smoking, a coping appraisal will consist of an individual's evaluation on whether giving up smoking is an effective way of avoiding severe disease (response efficacy), as well as an individual's ability to abandon smoking successfully (self-efficacy). Accordingly, the response cost can be regarded as any side-effects caused by giving up smoking (Arthur and Quester, 2004).

Protection Motivation is defined as an intervening variable which "arouses, sustains, and directs activity." (Rogers, 1975). It is the result of the threat appraisal and coping appraisal, which is also believed to heighten the engagement of actual adaptive behaviour. Researchers suggested protection motivation can best be measured by evaluating behaviour intentions (Boer and Seydel, 1996).

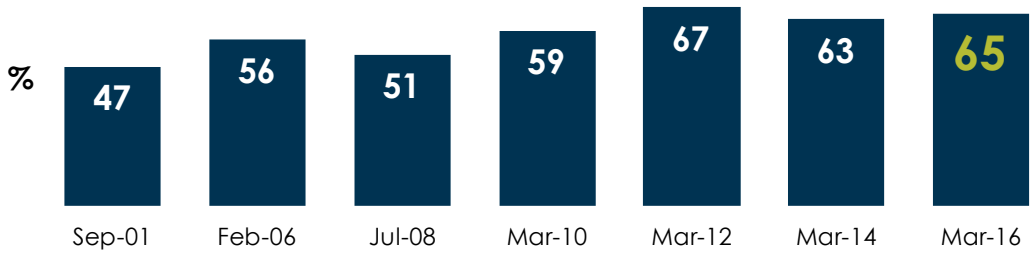
As the four most important components of the Protection Motivation Model (PMM), severity of harm, probability of occurrence (susceptibility), efficacy of the coping response and self-efficacy will be discussed in greater detail in the discussion of the conceptual model and hypotheses in Chapter 3.

2.4 Information Privacy Concern and Personalisation

Factors such as privacy concern and personalisation have been evaluated in prior research regarding Location-Based Service (Beresford and Stajano, 2013; Dinev et al., 2008; Xu et al., 2011). The trade-off between privacy concern and personalisation has been found to have significant impact on individual's behavioral intention. Since PMEAS is also a location-based service, the potential user's privacy concern and personalisation should also be examined alongside the PMT variables.

The increasing concern about individual privacy is an inevitable trend around the world. For example, according to New Zealand Privacy Commissioner's survey on New Zealander's privacy awareness in the past few years, the percentage of people who indicated "very concerned" about individual privacy has increased overall (Figure 3). In particular, those younger and more educated respondents showed more privacy concern than other participants. Privacy concerns are particularly noteworthy in an online environment due to the increasing significance of online threats, such as trojan, viruses, worms and spyware, etc. More than half of the internet users do not believe they can be completely anonymous online (Tsai et al., 2016).

Figure 3: Changes of "Very concerned" Over the Years
(New Zealand Privacy Commissioner, 2016)



Many studies have been done on privacy concern and human behavior in the Age of Information (Acquisti et al., 2015; Malhotra et al., 2004; Norberg et al., 2007; Xu et al., 2009; Xu et al., 2011) The relationship between privacy and other constructs has been examined by a number of empirical studies in the Information System (IS) area (Awad

and Krishnan, 2006; Chellappa and Sin, 2005; Kobsa, 2007; Xu et al., 2011). However, as it is not feasible to directly measure privacy, most IS empirical studies focus on privacy concern as the central construct, and use it as a measurable proxy for privacy. Some of the research focuses on the antecedents of privacy concern (with privacy concern as the dependent variable) while others focus on the outcomes of privacy concern (with privacy concern as the independent variable) (Dinev and Hart, 2003; Jarvenpaa et al., 1999; Malhotra et al., 2004; Xu et al., 2011). For example, researchers found that individuals who have been exposed to or been the victim of personal information abuses may have stronger concerns regarding information privacy (Norberg et al., 2007; Smith et al., 1996; Xu et al., 2011). On the other hand, a large body of research has explored the outcome of privacy concern. Among these studies, behavioral reaction and behavioral intention are the most prominent dependent variables that have been tested in relationship to privacy concern (Dinev et al., 2008; Lowry et al., 2011; Xu et al., 2009).

Previous research indicates that an individual's privacy concern with online services may be influenced by mismatched expectation (Rao et al., 2016). For instance, users may expect their personal information that is provided to a website can be deleted as they want, whereas the website may not allow the deletion of any data. Individual's privacy expectation (i.e. how their personal information will be collected, used and whether the information will be shared with other entities), may further depend on personal, social and cultural differences. Although some unexpected personal data practices will be notified in a privacy policy by most online service providers (e.g. e-commerce sites) based on compliance requirements, the common privacy policies are either too long to read, not written in natural language, or irrelevant to the user's current transactional context (Rao et al, 2016). Hence, it is easy to be ignored by the users, which eventually result in users exposing themselves to unexpected privacy risks, and in turn increase their privacy concerns.

Personalisation requires individuals to disclose their personal information. Personalisation is defined as "the ability to provide content and services based on knowledge about the individual (e.g. demographics, preferences, behaviour, needs.)" (Adomavicius and Tuzhilin, 2005; Xu et al., 2011). Recent advanced technology in information acquisition and processing allows online services to offer a diversity of web-based personalization that not only increases switching costs for users, but also

performs as an effective way to acquire valuable customer information. (Chellappa and Sin, 2005) In e-commerce, online companies track and collect customers' data (e.g. transaction history, searching and browsing data) to provide customized promotions on a strategic marketing purpose (Pavlou, 2011). This helps companies to fulfill their strategic purpose by offering customers prompt and personalised interaction (Kim and Lee, 2009). Therefore, it is widely recognized that personalisation is a service improvement that can increase both customers' satisfaction and companies' financial outcome (Zeithaml et al., 1996; Zeithaml et al., 2001). However, efforts and investments in online personalization may be undermined if consumers do not use these services due to their information privacy concerns (Chellappa and Sin, 2005).

Chellappa and Sin (2005) argued that a consumer is willing to share her preference information in exchange for obvious and immediate benefits, such as convenience, from using personalized products and services. Other researchers (Xu et al., 2011) also suggested there is a trade-off between personalisation and privacy concern when individuals are asked to disclose personal information and location data in exchange for the added value of receiving a message, which is personalised to their context, location, time of day etc. This is particularly relevant in the case of PMEAS, as the user-adaptive notification messages rely heavily on location data and other personalised data for the receivers to be effective. Hence, it is expected that perceived personalisation would significantly increase the user's satisfaction and intention to adopt personalised technology (Kim and Lee, 2009). In this study, personalisation refers to the use of a personalised emergency notification that is tailored to receiver's current situation (e.g. current location, health-status). At the same time, privacy concern about giving up personal information may act as an inhibitor of behavioral intention (Salleh et al., 2013). This leads to a trade-off between personalisation and privacy. Increased personalisation will mean giving up a degree of one's privacy. For this reason, it is important to consider the impact of personalisation alongside privacy concern in the research model.

2.5 Gaps in Prior Research

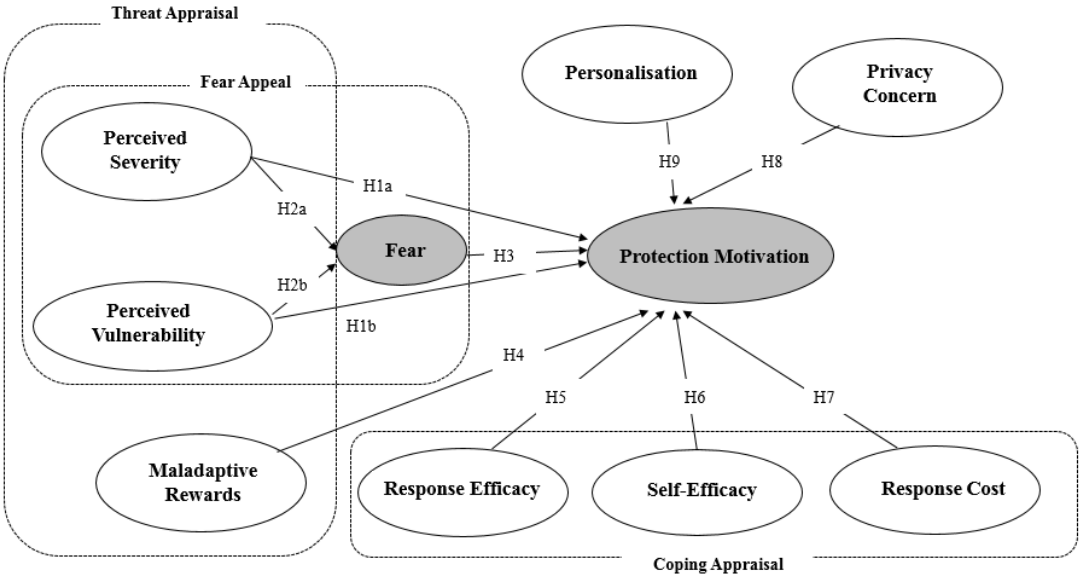
Prior research on emergency alert systems focuses on system design and information delivery (Báez et al., 2017; Hunter et al., 2007; Tupler and Mock, 2007). A few empirical studies have also been done to address an individual's intention to adopt such

systems (Aloudat and Michael, 2011; Haataja, et al., 2011; Wu et al., 2008). On the other hand, there is a large body of research on information disclosure and privacy which has primarily been interested in the trade-offs between perceived risks and benefits, and personalisation and the potential harm of privacy to customer (Chellappa and Sin, 2005; Dinev and Hart, 2006). A few of these studies have investigated individual's behavior in relation to personal information disclosure using PMT as a theoretical framework (Acquisti and Gross, 2006; Salleh et al., 2013). Salleh's (2013) study investigated the impact on individual's protection motivation, privacy concern, trust and perceived risk on their behavior in disclosing personal data in Social Network Sites (SNS). The result shows SNS users who perceive negative consequences or harm from disclosing personal data in SNS are more concerned over their online privacy. However, no studies have been found that examine motivation to use PMEAS that call on a person to disclose their personal information in order to receive personalised emergency alerts that aims to mitigate harm to an individual. Given the context is one in which use of PMEAS can help mitigate the impact of a threat and help protect one's well-being, it is expected that the context as well as other context-specific variables such as the likely emergency will result in different views of risk perception and willingness to disclose one's personal information in order to use a PMEAS. Given the research gap, this study builds on the Protection Motivation Theory, and incorporates the trade-off between privacy and personalisation to help explain individual's willingness to disclose personal information in the context of using PMEAS.

3. Model Development

Protection Motivation Theory has been used as a theoretical framework for explaining the influences on and predicting various behaviors, including health-related behaviour such as reducing alcohol use, enhancing healthy lifestyles, and preventing disease. (Boer and Seydel, 1996), and other behaviors such as individual self-disclosure on social network sites (Kim and Mousavizadeh, 2015), and increasing preparedness for earthquakes (Mulilis and Lippa, 1990). In the current study, Protection Motivation Theory (PMT) is used to frame the base model, that is the Protection Motivation Model (PMM) for evaluating protection motivation towards emergency threats. The PMM is extended by incorporating key privacy-related constructs (i.e. privacy concern and personalisation) to frame a conceptual model for explaining individual's willingness to disclosed personal information in the context of using PMEAS. It is assumed that consideration of privacy-personalisation trade-off, which is key to implementing a PMEAS, will impact protection motivation alongside key elements identified by PMT (e.g. perceived response efficacy, self-efficacy and response cost, etc.)

Figure 4: The Conceptual Model

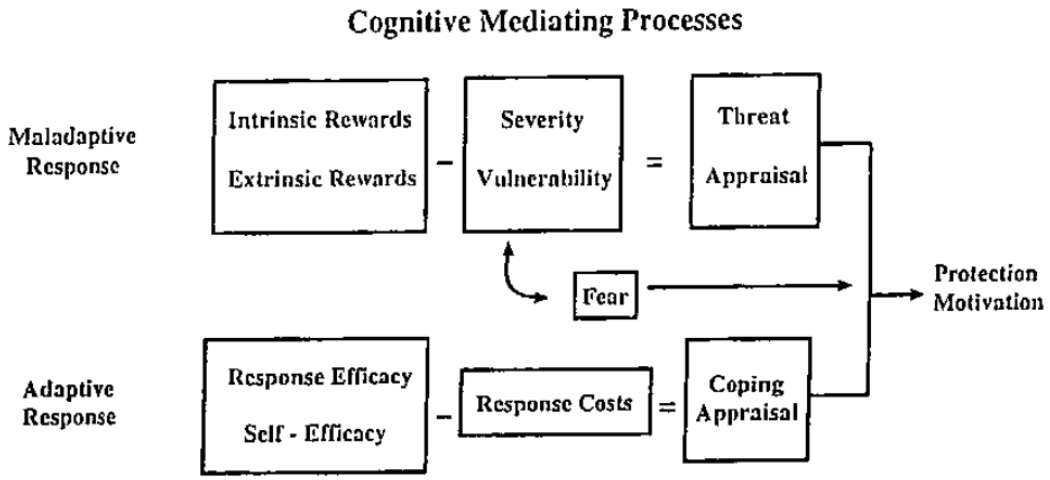


3.1 The Threat Appraisal

The revised PMT describes adaptive and maladaptive coping with a certain threat as the result of two parallel processes: a process of threat appraisal and a process of coping appraisal in which the behavioral options to mitigate the threat are evaluated (Floyd et al., 2000), as illustrated in Figure 5.

The threat appraisal process focuses on evaluating the components that are relevant to the threat. *Perceived severity*, *perceived vulnerability*, *maladaptive reward* and *fear* arousal are the four key components of the threat appraisal process. *Perceived Severity* evaluates the individual's belief on how serious the consequence of a threat would be to his or her well-being (Milne et al., 2000; Meso et al., 2013). It is typically measured by items such as "if my computer were infected by malware, it would be severe." (Johnston and Warkentin, 2010). *Perceived Vulnerability* refers to "how personally susceptible an individual feels to the communicated threat" (Milne et al., 2000). It is usually measured by items such as "It is likely that my computer will become infected with malware." (Johnston and Warkentin, 2010). As mentioned earlier, Rogers (1983) defined maladaptive rewards as perceived benefits of not performing the adaptive response to the threat event. Researchers (Floyd et al., 2000; Rogers and Prentice-Dunn, 1997) further categorised the sources of rewards into two different types (intrinsic and extrinsic), such as maintaining pleasure (intrinsic maladaptive reward) and saving money (extrinsic maladaptive reward).

Figure 5: A schematic representation of protection motivation theory (Floyd et al., 2000, p410)



Fear arousal is "a negatively valenced emotion representing a response that arises from recognizing danger, which may include any combination of. Apprehension, fright, arousal concern, worry, discomfort and negative mood." (Boss et al., 2015). The typical measurement usually uses measures of different extent of fear feelings such as "I am worried/frightened/ anxious/scared about the prospect of losing data from my computer." (Milne et al., 2002). In the case of a threat-response behavior (e.g. to reduce chance of contracting a disease), perceived vulnerability (e.g. estimates the chance of contracting a disease) and perceived severity (e.g. estimates the seriousness of a disease) are expected to motivate the adaptive response to mitigating the threat, and at the same time to inhibit the maladaptive response that places an individual at risk (Floyd et al., 2000). Fear arousal impacts positively the protection motivation by intensifying perceived severity and perceived vulnerability of a threat.

Researchers argue that the relationship between varying levels of depicted severity of a threat and the persuasion of the message is positive and linear (Arthur and Quester, 2004). In Rippetoe and Rogers's (1987) study, manipulation checks were conducted among the subjects who received written messages containing a high versus low threat essay about breast cancer (which varied the depicted severity of and vulnerability to breast cancer). The results revealed that perceived severity of the disease is significant in relation to the intention to perform a breast self-examination. In Boss et al. (2015)'s study regarding the use of anti-virus software, participants who were provided with a high risk message were found to have much stronger intentions to use anti-virus software than those who were provided with low risk message. Thus, an individual's perceived severity of a threat tends to be positively linked to their intention to perform the protective actions (Ifinedo, 2012).

Similar to the health-related information that describes a threat that may be harmful to an individual's internal well-being, an emergency notification by PMEAS also describes an emergency threat that can potentially result in harm to an individual's well-being. Given the nature of the threat, we propose that an individual would similarly perform a threat appraisal in the context of PMEAS. It is expected that if individuals perceive an emergency situation to be a threat that could lead to potential damage to themselves, they are more likely to consider following the guides and requirements to mitigate the threat (Ifinedo, 2012; Pechmann et al., 2003). It is also expected that there is a positive relationship between perceived severity and behavioral intention in the context of PMEAS. The more serious the individuals perceives the consequences

resulting from an emergency to be, the more they are willing to adopt the adaptive actions (Lee, 2011). Therefore, perceived severity of the emergency threat is expected to motivate the adaptive response (i.e. to use a PMEAS by disclosing personal information), and enhance the protection motivation in the context of using PMEAS. The following hypothesis is proposed:

H1a: Perceived Severity of an emergency threat is positively related to Protection Motivation to use a PMEAS.

The perception of vulnerability has been found to be related to individual's evaluation on his or her probability of exposing to a painful threat (Woon et al., 2005). Some research findings demonstrated that perceived vulnerability has a significant impact on behavioral intention to take protective actions (Ifinedo, 2012; Lee and Larsen, 2009). In Wurtele's study (1988), a group of female students who had been provided with information about osteoporosis showed a strong belief in their vulnerability to osteoporosis, which in turn, had a significant positive relationship to their intention to increase calcium-rich food.

At the same time, perceived vulnerability has been found to be an inconsistent predictor in some studies. While some studies supported the positive relationship between perceived vulnerability and behavioral intention (Cismaru and Lavack, 2006; Ifinedo, 2012; Lee and Larsen, 2009; Lee, 2011), others did not (Johnston and Warkentin, 2010; Yan et al., 2014). One of the possible reasons is because the context varies in experimental research, such that the performance of a specific experimental task may differ from another (Crossler et al., 2014). In our study, we apply the full nomological model with all the variables initially in the revised PMT model. Thus, consistent with the PMT, we argue that perceived vulnerability is positively related to behavioral intention.

According to PMT, it is expected that an individual would perform a threat appraisal when using PMEAS, and therefore the assessment of an individual's vulnerability (e.g. the chance of being impacted by a severe earthquake that causes damage) is expected to motivate their protective behavior intention so as to mitigate the potential threat. For example, with respect to being willing to use a PMEAS, that is to receive protective information provided by a PMEAS, individuals who view themselves as more vulnerable to possible emergencies such as earthquake and floods are more likely to

use PMEAS. Consequently, it is expected that they will be more willing to take protective actions (i.e. subscribing to a PMEAS) if they perceive their vulnerability to an emergency to be high. Thus, we propose the following hypothesis based on the previous research:

H1b: Perceived Vulnerability of an emergency threat is positively related to Protection Motivation to use a PMEAS.

According to the revised Protection Motivation Model (Rogers, 1983), fear is a necessary outcome of the threat appraisal (i.e. when the threat appraisal to be high). Along with a coping appraisal, the two cognitive processes mediate the persuasive effects of a fear appeal by arousing protection motivation (Maddux and Rogers, 1983). Research also proposed fear as a mediating variable between the vulnerability and behavioral intention, and between the severity of the threat and behavioral intention (Arthur and Quester, 2004). A group of prior studies support the positive relationship between fear and protection motivation (Arthur and Quester, 2004; Boss et al., 2015; Plotnikoff and Higginbotham, 2002). For example, Arthur and Quester's study (2004) found the emotional response of fear was a significant indicator of behavioral intention when participants were provided with advertisements that contained threatening messages. The research conducted by Boss et al. (2015), on the other hand, supported the strong significant relationship between perceived threat severity and perceived threat vulnerability to fear in a high fear appeal context, as well as a moderate significant relationship between the same constructs in a low fear appeal context.

In using a PMEAS, an emergency notification usually describes the threat of an impending danger or harm (Aloudat and Michael, 2011), which can be regarded as a fear appeal communication used in an attempt to persuade receivers to take protective actions. It is expected that the more vulnerable an individual feels to an emergency and the more serious he or she thinks it to be, the greater the fear that will be aroused and the stronger the threat appraisal will be (Milne et al., 2000). Accordingly, a greater threat appraisal of the emergency will in turn motivate the individual to take protective responses. Hence, we propose a positive relationship between fear and protection motivation. We also propose a positive relationship between perceived severity and perceived vulnerability to the emergency threat, and fear based on the previous research (Arthur and Quester, 2004):

H2a: Perceived Severity of emergency threat is positively related to Fear.
H2b: Perceived Vulnerability of emergency threat is positively related to Fear.
H3: Fear of an emergency is positively related to Protection Motivation to use a PMEAS.

Maladaptive rewards refer to any kind of rewards for the response of not protecting oneself from the threat (Boss et al., 2015). For example, in the context of coping with a health threat such as breast cancer, a maladaptive reward can be the reduction of stress from avoidance or wishful thinking about breast cancer (Rippetoe and Rogers, 1987). Previous research found that if the maladaptive rewards overweigh the perceived threat, a person may tend to choose the route of not following the desirable protective behaviour (Boss et al., 2015). A PMEAS is expected to target the receivers in a precise and timely manner, but this may run the risk of receiving false alarms or irrelevant notifications (Seaborn, 1975). Research pointed out that some communities had a high mistrust towards early warning systems such as PMEAS since it previously produced predictions of emergency that did not materialize (Lucy Pearson, 2012). Another study also found that people who previously experienced "riding out" emergencies are likely to feel complacent when receiving warning messages (Wilde, 2013). Maladaptive rewards in a PMEAS context may therefore be expressed as people's wishful thinking about an emergency situation from an intrinsic perspective such as thinking they will not get hurt by a potential emergency, or from an extrinsic perspective such as thinking that not using PMEAS may help to avoid false alarms or irrelevant notifications. Advantages of maladaptive behavior therefore facilitate the probability of a maladaptive response, which performs as an inhibitor to protection motivation (Boer and Seydel, 1996). As such, we propose:

H4: Maladaptive Rewards is inversely related to Protection Motivation to use a PMEAS.

3.2 The Coping Appraisal

As illustrated in Figure 5, response efficacy, self-efficacy and response cost are the key components of coping appraisal. These components concern evaluating the expectation that carrying out the recommended actions can mitigate the threat (response efficacy) and the belief in an individual's ability to execute and complete the action successfully

(self-efficacy), alongside any potential cost to the individual of carrying out the adaptive behavior (Boer and Seydel, 1996).

Response efficacy is the degree to which a person believes that the recommended response will be effective (Maddux and Rogers, 1983). As a cognitive process, individual's cognitions of response efficacy will ultimately drive them to decide the manner in which they would like to address the threat (Rogers, 1983). In existing empirical studies using PMT, response efficacy is shown to be one of the best predictors of behavioral intention regardless of the research context (Boer and Seydel, 1996; Boss et al., 2015; Crossler et al., 2014; Ifinedo, 2012; Lee, 2011; Wurtele, 1988). It is typically measured by items such as "Anti-virus software is effective in removing the virus" (Anderson and Agarwal, 2010; Johnston and Warkentin, 2010). In Wurtele's empirical study (1988) of female students' perceptions about osteoporosis and behavioral intention, response efficacy was identified as the second-best predictor of the subject's intention to increase calcium-rich food in the diet. In another study regarding anti-plagiarism software adoption (Lee, 2011), response efficacy was found to be the only construct in the coping appraisal that has a direct significant impact on the actual adoption. In other studies using PMT such as employees' intention to follow Bring Your Own Device (BYOD) policies (Crossler et al., 2014), and intention to adopt appropriate information security actions among college students (Meso et al., 2013), response efficacy has a consistent significant effect in predicting the behavioral intention, as well as actual behavior.

Similarly, using a PMEAS can be expected to help persons effectively mitigate a threat by taking the appropriate actions. For instance, a tornado hit in New York heavily damaged more than 20 homes. However, no significant injuries resulted since most of the residents had subscribed to local PMEAS, and were able to take shelter in their basements upon receiving an alert on their cell phones (National Ocean and Atmospheric Administration, 2016). According to PMT (Rogers, 1983), a higher level of response efficacy is found to be positively associated with the protection motivation to mitigate the threat whereby adaptive actions are taken. With respect to an individual's behavioral intention of adopting PMEAS as a way to help mitigate potential threat, he or she will consider the utility of disclosing personal information to use a PMEAS based on their response appraisal (Johnston and Warkentin, 2010). It is also reasonable to expect that individuals who have a high degree of response efficacy in the context of PMEAS would demonstrate stronger intentions to use the service by

engaging in sufficient information disclosure in exchange for personalised notification (Lee, 2011). Thus, it is with this research background that we propose the following hypothesis:

H5: Response Efficacy is positively related to Protection Motivation to use a PMEAS.

Self-efficacy refers to "the belief of the subject that the recommended behaviour can be executed successfully." (Boer and Seydel, 1996). In other words, it is "the belief that a person is or is not capable of performing a coping behavior." (Lee, 2011). Self-efficacy is usually measured by items that are related to an individual's capability of performing a task, such as "I have the necessary skills to protect myself from information security violations", and "I believe that it is within my control to protect myself from information security violations" (Ifinedo, 2012).

Researchers in self-efficacy believe that psychological change is largely manipulated by the transformation of individuals' expectations of their mastery of a given behaviour or task (i.e. the belief of individual's capability of performing the behavior) (Maddux and Rogers, 1983). In health-related and IS-related (Information System) empirical studies using PMT, self-efficacy has been shown as a promising predictor of behavioral intention (Boer and Seydel, 1996; Crossler et al., 2014; Prentice-Dunn et al., 2009; Ifinedo, 2012). The study by Fruin et al. (1991) revealed high self-efficacy expectancy resulted in the stronger endorsement of the behavioral intention. In another quantitative study conducted by Ifinedo (2012), participants who had a higher level of self-efficacy were more willing to comply with information system security policy (ISSP) than those who had lower level of self-efficacy.

In the context of a PMEAS, self-efficacy primarily refers to the user's ability to use the PMEAS mobile application. Similar to the cognitive process that an individual engages in assessing their response efficacy which eventually drives his or her behavioral intention (Johnston and Warkentin, 2010), evaluating self-efficacy as an individual's confidence in their ability to use and maintain a PMEAS is also an important part of determining the behavioral intention. Hence, self-efficacy in using a PMEAS is expected to be positively related to an individual's protection motivation (i.e. behavioral intention to use a PMEAS). If individuals assess their own capability to use the service (e.g. install the mobile application, maintain the personal profile in the

application (Johnston and Warkentin, 2010)) to be high, they are more likely to disclose personal information to use a PMEAS. Therefore, we propose the following hypothesis based on the above arguments:

H6: Self-Efficacy is positively related to Protection Motivation to use a PMEAS.

Response costs are any perceived personal costs triggered by adaptive responses such as costs related to money, effort and time. (Boss et al., 2015). For example, "A person may be isolated if he or she does not smoke" (Yan et al., 2014); "There are too many overhead costs associated with implementing IS security measures in my organization" (Ifinedo, 2012). A coping appraisal weighs response efficacy and self-efficacy against perceived costs. The cost of carrying out an adaptive behaviour then limits protection motivation (Boer and Seydel, 1996).

Similar to perceived vulnerability, response cost is found to be an inconsistent predictor of behavioral intention. Some studies support its positive relationship with behavioral intention (Lee and Larsen, 2009; Rahaei et al., 2015; Woon et al., 2005), while others do not (Crossler et al., 2014; Ifinedo, 2012). For instance, Rahaei et al. (2015) conducted a study in Cancer Early Detection (CED) behaviors. The results showed that despite the strong response efficacy and self-efficacy in CED, costs associated with CED performed as a key barrier to engaging in the actual behavior, particularly among women with low income and socio-economic status. On the other hand, Ifinedo's (2012) study found that there was no negative relationship between response cost and compliance intention to the Information System Security Policy (ISSP). In explaining these results, Ifinedo (2012) suggested this may be due in part to research design and the composition of participants such that some participants may have a positive view of the cost-benefit of complying with IS security policy, while others may have a different perspective. For example, if the response cost is high, even if the benefits are also high, this may result in non-action.

As a cost of using a PMEAS, in some contexts users must pay to receive the notification. There may also be other costs such as charges for data usage and time and effort related to updating personal information such as health status and location details. Consistent with fundamental research in PMT, we argue that the perceived cost of using a PMEAS may limit protection motivation. It is expected that if an individual perceives the

response cost to be high, he or she will be less willing to use a PMEAS (Crossler et al., 2014). Hence, we propose the following hypothesis:

H7: Response Cost is inversely related to Protection Motivation to use a PMEAS.

3.3 The Privacy-Personalisation Trade-off

Previous research proposed that the collection of a significant amount of personal data (e.g. 24*7 location data) for personalised services may impact the individual's privacy concern (Beresford and Stajano, 2013). For example, Dinev's (2008) study further showed that individual's privacy concern performs as an inhibitor in online e-commerce, which is negatively associated with their willingness to disclose personal information in online transactions. In the context of PMEAS, location data from users' mobile devices are continuously being collected (Weng, 2003). Given prior research outcomes of a negative relationship between privacy concern and willingness to disclose personal information to use an online service, it is expected that individuals who have a higher privacy concern in relation to the use of PMEAS (such as thinking the PMEAS provider is collecting too much data from users, or being worried about the misuse of personal information) will be less willing to disclose personal information to PMEAS. Hence, we propose the following hypothesis:

H8: Privacy Concern is inversely related to the willingness to disclose personal information to use a PMEAS.

The prior research shows that personalization can be a motivation for users to disclose their personal information in exchange for personalized services and/or information access (Xu et al., 2011). Personalization is obtained when users receive information that is tailored to their location, context, and other personal identities (Junglas and Watson, 2006). Companies continue to adopt personalised service because of the benefits their businesses received from a personalisation strategy (Awad and Krishnan, 2006). On the other hand, customers received benefits from personalised service such as greater efficiency and convenience which may increase their intention to purchase items or use the services of these companies (Lee and Cranage, 2011).

In the case of PMEAS, personalisation would allow notification providers to provide personalised emergency alerts for mobile users, such as notification of an impending emergency within 50KM to users' current location, or specific instructions for protecting a user from an emergency situation based on his or her personal profile (e.g. disabilities). Hence, it is expected that an individual's perception of the potential benefits provided by a personalised PMEAS will motivate them to disclose personal information in exchange for the notifications from PMEAS. We therefore propose the following hypothesis:

H9: Personalisation is positively related to the willingness to disclose personal information to use a PMEAS.

3.4 Control Variables

Previous research indicates that interpersonal differences such as gender, age and education may influence behavioral intention to engage in adaptive responses (Boer and Seydel, 1996; Crossler et al., 2014; Kim and Mousavizadeh, 2015; Lee, 2011; Rahaei, 2015; Yan et al., 2014). For example, in a research of consumer decision-making using PMT, men were found to differ from women in their perceptions of self-efficacy and response cost (Cismaru and Lavack, 2006). Studies in information privacy also suggested interpersonal difference has an impact on individual's willingness to disclose information to use a personalised online service (Bansal et al., 2016; Xu et al., 2011). For example, people with higher personal innovativeness are more likely to accept a new technology (Xu et al., 2011). However, other research findings did not support the argument that these variables influence individual's behavioral intention (Melamed et al., 1996; Milne et al., 2002).

Given the inconclusiveness of the prior research and the knowledge that different factors may influence PMT in different ways due to the differences in context or among participants, in this study control variables such as gender, age, education, geographical location and innovativeness are tested to evaluate their impact in the main model. This is further discussed in the Data Analysis chapter.

3.5 Chapter Summary

In conclusion, Figure 4 presents the research model. In this model, we examine individuals' protection motivation, which is conceptualized in this study as willingness to disclose personal information in the context of PMEAS. This model applies all the variables in the revised Protection Motivation Model (Rogers, 1983). We also argue further that individuals' privacy concern and personalisation will have a significant impact on willingness to disclose personal information in order to use a PMEAS.

4. Research Methodology

This chapter first explains the research methodology and research approach adopted in this study. It is followed by a description of the vignettes that are used in the survey. After that, the development of survey questions and construct measures is discussed.

4.1 Methodology and Epistemology

This research takes a positivist approach. A positivistic epistemology is objective, believing that knowledge of reality exists beyond the human mind. (Chua, 1986; Weber, 2004). The role of researchers in this research context is to test theories within a hypothetical-deductive mode (or a scientific method) to seek the truth.

4.2 Research Design and Method

This study uses a quantitative research approach that combines the traditional survey with the vignette technique. "Vignette studies use short descriptions of situations or persons (vignettes) that are usually shown to respondents within surveys in order to elicit their judgments about these scenarios." (Atzmüller and Steiner, 2010). Since most of the respondents have no experience of using PMEAS, this approach is ideal for describing the technology and circumstances under which PMEAS may be used in real life situations, in order to identify and clarify the respondents' complex beliefs and decision-making process regarding its use.

The survey was conducted in New Zealand with across a range of respondents differing in gender, age, education, ethnicity, and geographical region. The targeted participants were mobile users who were 18 years and above. Two hypothetical scenarios (vignettes) were designed with the New Zealand's context in mind.

Before conducting the survey, a draft of potential survey questions was prepared and reviewed by two academics to determine their appropriateness for the survey including the wording of the questions, the measurement scales and the survey administration process. Following the review, an application for human ethics approval was submitted to the University of Canterbury Human Ethics Committee. After the application was

approved, a pre-test was conducted with a convenience sample of 30 mobile users in New Zealand, which included students of the University of Canterbury and employees in New Zealand companies. Based on the results and feedback received from the pre-test, some of the terminologies used in the survey and wording of the questions were further refined to ensure a better understanding for potential respondents in the formal survey.

Supported by Qualtrics (https://canterbury.qualtrics.com), an online survey was used for data collection. Access to the survey was provided through the Qualtrics survey service to help recruit participants that met the survey requirements. No personally identifying information was collected in the survey, thus maintaining the confidentially of survey participants' identities.

As a part of the survey implementation, to assure the quality of the responses, three quality check settings were adopted, responses that failed to pass the quality check were eliminated for future data analysis:

1. *Survey Validation*. "Force Response" settings were used for all the questions that related to the model constructs.

2. *Attention Filter*. Two attention filter questions were used in the survey. These questions asked respondents to select "Strongly Disagree" for these statements.

3. *Survey Duration*. The speed check setting enforced a minimum time for taking the survey. This means that respondents who attempted to take the survey in less than 1/3 the average time were excluded from the set of valid responses.

4.3 Fear-Appeal Manipulation

To manipulate fear appeal, the survey presented two emergency scenarios (vignettes). Both scenarios described emergencies that would be familiar to the target population, and which have had widespread impacts within New Zealand in the last 7 years. Although they did not explicitly indicate the potential severity or susceptibility of the situation for the individual, the descriptions were of such that they targeted situations

that could have a significant impact. Scenario #1 (Storm) described a storm emergency with potential for flooding.

> *"The National Weather Service issues a storm watch for parts of your country, which includes your region. Heavy rains have been falling for three hours. The storm system is moving towards where you live. High winds and flooding have been reported in some areas."*

Scenario #2 (Earthquake) depicted a strong earthquake causing damage, which was close to the participant's location:

> *"A magnitude 6.0 earthquake happened about 20km from your location (at a depth of 10km). Strong ground shaking from the main shock lasted for approximately 45 seconds in some areas. Aftershocks of varying intensity will be felt throughout the region for several days following the main shock, causing further damage to structures that were already damaged or weakened by the previous shaking."*

These scenarios are especially relevant to the New Zealand context. While the lower north island and south island have experienced strong earthquakes in the last 7 years, different parts of the north island and parts of the south island have been subject to major flooding. For Scenario #1 (Storm), New Zealand has experienced many episodes of heavy flooding. The most recent (April 2017) included a '500-year event' in Edgecumbe (north island) due to a storm producing around three times the normal April rainfall within three days. This flooding resulted in an evacuation that affected 580 households and approximately 1600 people (Stuff, 2017). In March 2016, over 200 persons were evacuated on the West Coast following wild weather, and in June 2015, more than 400 persons were evacuated after major floods affected the lower North Island. For Scenario #2 (Earthquake), there have been four major earthquakes in the last 7 years resulting in serious long-term damage across wide areas (e.g. Christchurch 2010 and 2011; Wellington 2013, Kaikoura 2016), with 185 fatalities in the 2011 Christchurch earthquake. These four events have been concentrated in the lower north island and Canterbury region in the south island. Compared with flooding where the consequences of damage have been more localized, the earthquakes have had more widespread impacts and damages, affecting thousands of people.

4.4 Survey Development

Appendix B provides the survey questions used in this research. The survey comprised of four parts.

In the first part of the questionnaire, a brief introduction to the background and purpose of the research is provided. The first part also highlighted the assurances of confidentiality and anonymity, and other statements about participation as required by the University of Canterbury Human Ethics Committee. This section also provided definitions of terms that are used in the survey.

Next, respondents were asked about their experience with mobile device use, including the use of location-based services and to Personalised Mobile Emergency Alert Services (PMEAS).

This was followed by the scenario-based questions aimed to assessing ear appeal. For each scenario, participants were asked to respond to questions related to their risk perceptions of the situation, that is, perceived severity, perceived vulnerability, and fear. All the participants were asked to answer questions for both scenarios. Respondents then responded to questions on their willingness to disclose personal information to use a PMEAS, and their perceptions in relation to response efficacy, self-efficacy, response cost, personalisation, privacy and other beliefs that are associated with PMEAS use. All responses in this section were captured using 7-point Likert scales with "Strongly Disagree -3" and "Strongly Agree +3" as the end points.

Finally, respondents were asked to provide some demographic information such as their gender, age group, highest level of education achieved, geographical area, and ethnicity to be used for descriptive statistical purposes.

4.5 Operationalization of Constructs

The development of the survey items was based on the existing literature (see Appendix C).

Threat appraisal measures. The following measures of perceived severity, perceived vulnerability, fear and maladaptive rewards were used to assess PMT's threat appraisal components. To measure *perceived severity* of a depicted emergency, participants responded to five statements adapted from Milne et al. (2002) and Johnston and Warkentin (2010), for example: "If I were affected by an emergency situation like this, it would be severe".

Three items adapted from John and Warkentin (2010), and one item adapted from Milne et al. (2002) were used to measure respondent's *perceived vulnerability* for each emergency scenario. For example: "It is likely that I will be affected by an emergency situation like this."

Participant's *fear* perception in each emergency scenario was assessed using four items adapted from Milne et al. (2002). For example: "The prospect of being affected by an emergency like this would make me worried." Questions for perceived severity, perceived vulnerability and fear were repeated for both scenarios.

Three items were adapted from Myyry et al. (2009) to measure *maladaptive rewards.* For example: "Not using a PMEAS would save me time." The other three indicators for maladaptive rewards were newly created based on an understanding of PMEAS. These included "Not using a PMEAS would avoid false alarms/save me from taking unnecessary actions/avoid unnecessary disruption.

Coping appraisal measures. The following measures of response efficacy, self-efficacy and response cost were used to assess PMT's coping appraisal. To measure response efficacy, three items adapted from Johnston and Warkentin (2010) were used and modified to suit the research context. For example: "Using a PMEAS would be a good way to reduce my risk of being affected by an emergency situation."

For *self-efficacy*, three items were adapted from Meso et al. (2013) and Ifinedo (2012). One of the sample items is "I have the resources to use a PMEAS".

Four items adapted from Myyry et al. (2009), Woon et al. (2005) and Ifinedo (2012) were used to assess respondent's perception of response costs that are associated with using PMEAS use. For example, "Using a PMEAS would require considerable investment of effort other than time." The other two indicators were adapted from Meso

et al. (2013) and tailored to the PMEAS context. The two items are "It would be time-consuming to set up a PMEAS (e.g. providing my personal data such as name, address, health information, etc.).", and "It would be time-consuming to maintain my personal profile in a PMEAS (e.g. updating my mobile number, address, health information, etc.).

The items to assess privacy and personalisation trade-off were also adapted to the PMEAS context from prior literature. Privacy concern was measured using items from Malhotra et al. (2004) and Li et al. (2011). For example, "I would be concerned that a PMEAS provider would be collecting too much information about me."

Items for personalisation were adapted from Xu et al. (2011) to the research context. The three items highlight the participant's perception of PMEAS services in providing an emergency notification that is specific to the user's context, preference or personal needs. For example, "A PMEAS could provide me with emergency alert information that is tailored to my personal needs."

Finally, *protection motivation* was measured using behavioral intention as a proxy, which in this case is participant's willingness to disclose personal information to use a PMEAS. The items were adapted from Milne et al. (2002). For example, "If personalised Mobile Emergency Alert Service (MEAS) were available, I intend to use a PMEAS."

5. Data Analysis

5.1 Descriptive data of participants

The survey received 424 responses of which 261 of were valid responses. 163 responses were excluded either because the participants did not meet the selection criteria for participating in the survey, or they did not meet the quality checks, that is, they did not pass the speed check or attention filters. The result shows that 139 responses failed to pass the attention filter checks (i.e. "Please select 'Strongly Disagree' for this statement.") and 2 responses failed to pass the speed check. 13 of the potential respondents did not use mobile devices, 3 persons did not meet the age requirement (i.e. 18 years or above), and 5 persons were outside New Zealand. These persons were also excluded from the survey.

Following the above exclusions, the survey received a total of 261 valid responses (See Table 1). Of those who indicated their gender (99%), 44% of the respondents were male and 55% were female. Around 34% of the respondents were aged from 18 to 34, 33% from 35 to 49 years and the remaining 33% were 50 years and above. Of those who indicated their education background (99%), 40% of the participants indicated that they had an undergraduate degree or above. Approximately one third had a tertiary or some undergraduate qualifications (34%). The remainder (25%) had other qualifications such as primary school, secondary school qualification and apprenticeship. For the ethnic groups, 72% of the participants were New Zealand European, 6% were Māori and 5% were Indians. The rest of the respondents (20%) covered a diversity of ethnical groups including Samoan, Cook Island Māori, Chinese, European American, Other European, Latin American, Russia, South Africa, Malaysian, Thai, Vietnamese, Filipino and Korean. In terms of the geographical region, most respondents were from the major regional areas of Auckland (30%), Wellington (13%) and Canterbury (13%). Approximately 74% of the respondents were from north island while 26% were from the south island. Also, 81% of the respondents were living in an urban area while 19% were living in rural areas.

Table 1. Demographic Statistics of Participants

Demographic Variable (n=261)	Frequency	Percentage (%)
Gender		
Male	115	44%
Female	144	55%
Other/Prefer not to say	2	1%
Age		
18-24	37	14%
25-29	28	11%
30-34	24	9%
35-39	32	12%
40-49	54	21%
50-59	45	17%
60 and above	41	16%
Education (3 missing)		
Primary School Qualification	4	2%
Secondary School Qualification	52	20%
Tertiary Certificate	35	13%
Tertiary Diploma	34	13%
Some Undergraduate Degree Study	22	8%
Undergraduate Degree	71	27%
Postgraduate Degree	33	13%
Other (e.g. Private School, Apprenticeship)	7	3%
Ethnic Group		
New Zealand European	187	72%
Māori	15	6%
Samoan	2	1%
Cook Island Māori	2	1%
Chinese	6	2%
Indian	12	5%
Other (e.g. Other European, Latin American, South Africa, Russia, Malaysian)	46	18%

Geographic Region (1 missing)		
Northland	8	3%
Auckland	79	30%
Waikato	22	8%
Bay of Plenty	13	5%
Hawkes Bay	10	4%
Taranaki	5	2%
Manawatu/Whanagui	19	7%
Wellington	35	13%
Nelson/Marlborough/West Coast	7	3%
Canterbury	33	13%
Otago/Southland	28	10%
Other (Masterton/Wairarapa)	1	<1%
Area (2 missing)		
Urban area	212	81%
Rural area	47	18%

Examining the information related to respondents' mobile use shows that a large proportion of people were long-time mobile device users (67%) having used mobile devices for 10 years or more. The majority (75%) were using WIFI frequently. In addition, nearly half of the respondents (49%) were using mobile data frequently while another 26% used it sometimes or occasionally. Only 13% rarely used or did not use (12%) mobile data.

Table 2. Mobile and LBS Use of Participants

Demographic Variable (n=261)	**Frequency**	**Percentage (%)**
Mobile use (years)		
1-4 years	21	8%
5-9 years	64	25%
10 years and more	176	67%
Wi-Fi use		
Always/Very Often/Often	196	75%
Sometimes/Occasionally	21	8%

Rarely	16	6%
Never	28	11%
Mobile Data Use		
Always/Very Often/Often	129	49%
Sometimes/Occasionally	68	26%
Rarely	33	13%
Never	31	12%
Location-Based Services (LBS) Use		
Always/Very Often/Often	85	33%
Sometimes/Occasionally	85	33%
Rarely	49	18%
Never	42	16%

Location-Based Services (LBS) are applications that use one's location (e.g. GPS data) to provide information that is tailored to specific to that location.

The results (Table 2) also show that Location-Based Services (LBS) are widely accepted and used in New Zealand. Only 16% of the respondents have never used LBS whereas one third of them (33%) were using LBS on a frequent basis, and another 33% were using it sometimes and occasionally. Only 18 of the respondents (7%) indicated they were using a PMEAS (Table 3). These included Civil Defense, Geonet, Hazards/Red Cross, Info Alert and Wireless Emergency Alerts. For 13 respondents, the PMEAS were pushing notifications based on their current location.

Table 3. PMEAS Use of Participants

Demographic Variable (n=23)	**Frequency**	**Percentage (%)**
PMEAS use		
Yes	18	7%
No	243	93%
Frequency of PMEAS use		
Always/Very Often/Often	7	39%
Sometimes/Occasionally	9	50%

Rarely	2	11%
Location Based PMEAS		
Yes	12	67%
No	6	33%

The respondents were also asked to indicate the types of information they would be willing to disclose to a PMEAS. The results (See Table 4) suggests that the majority of respondents (80% and above) would be willing to disclose their mobile phone number, email address, name and town or city. 76% of the respondents would also disclose their mobile GPS location to a PMEAS, which is most essential information needed for a PMEAS to send personalised emergency notification based on user's current location. The result also showed that fewer persons would be willing to disclose more personal information such as information about a disability (66%), heath information (58%), or their home address (61%). The information that respondents would be least likely to disclose includes their home and work phone number, and their personal statistics such height and weight.

It is notable that apart from the information listed in the questionnaire that covered personal details, contact details, health-related information and location information, some participants also added that they would like to provide other information such as their pet's information and a photograph.

Table 4. Types of Information That Persons Are Willing to Disclose to a PMEAS

Type of Information	**Frequency**	**Percentage (%)**
(Mobile) Phone Number	240	92%
Email Address	218	84%
Name	214	82%
Your Town or City	208	80%
Gender	206	79%
Age	204	78%
GPS Location of Mobile	199	76%
Household Composition and Relationships	194	74%
Postal Code or Suburb	193	74%

Emergency Contact	182	70%
Disabilities	173	66%
Home Address	159	61%
Health Information	151	58%
Registered Location of Interest	141	54%
Registered Location of Family and Friends	133	51%
(Home) Phone Number	120	46%
Body Statistics	97	37%
(Work) Phone Number	65	25%

5.2 Fear Manipulation Check

In order to check whether fear appeal makes a difference to participant's perceptions of emergency situations, a t-test was used to check the difference within subject means (See Table 5). Differences in perceived severity, perceived vulnerability and fear were significant ($p<0.05$), with participants reporting stronger perceived severity, perceived vulnerability and fear in Scenario #2 (Earthquake) than in Scenario #1 (Storm). Results therefore showed that fear appeal for Scenario #2 (Earthquake) was greater than Scenario #1 (Storm) across three variables related to fear appeal (i.e. perceived severity, perceived vulnerability and fear).

Table 5. Fear Manipulation Check Using T-test

Construct	**Scenario**	N	Mean	Std. Deviation	t	Sig.
Perceived Severity	#1 (Storm)	261	4.7	1.33	-9.593	.000
	#2 (Earthquake)	261	5.7	1.08		
Perceived Vulnerability	#1 (Storm)	261	4.4	1.40	-6.793	.000
	#2 (Earthquake)	261	5.2	1.28		
Fear	#1 (Storm)	261	4.2	1.60	-6.914	.000
	#2 (Earthquake)	261	5.2	1.45		

5.3 Evaluation of Outer (Measurement) Model

In this research, we use the Partial Least Squares (PLS) approach to path modelling to examine the research model. The PLS approach is a variance-based approach to structural equation modelling that has been widely used to evaluate the use of new technologies, including the use of location-based mobile technologies and services (e.g. Xu et al., 2011; James et al., 2015). It is especially suited when the goal of the research is to predict the 'target' construct and identify key 'driver' variables (Hair, et al., 2014). It is also suitable when the research model is relatively complex (e.g. there are many constructs) relative the size of the sample, and includes both reflective and formative constructs (Hair, et al., 2014). The research data is analysed using Partial Least Square (PLS) method using SmartPLS (Version 3.2.6) software package.

In this section, the measurement model is examined in terms of measurement reliability and validity. For the research model, two constructs (cost, maladaptive rewards) are modelled as formative (composite) models, while the others are modelled as reflective (common factor) models.

5.3.1 Reflective (Common Factor) Variables

To assess the reflective constructs of the model, this study uses item loadings to evaluate individual indicator reliability, Composite Reliability (CR) and Cronbach's Alpha to examine internal consistency, and Average Variance Extracted (AVE) to assess convergent validity (Hair et al., 2017).

The result of internal validity checks (Table 6) show that Composite Reliabilities (CR) ranged from 0.898 to 0.967, while Cronbach's Alpha ranged from 0.833 to 0.955. Both exceeded the recommended threshold of 0.70 so were regarded as satisfactory (Chin et al., 2010). Convergent validity indicates the extent to which items positively correlate with interchangeable measures of the same construct (Hair et al., 2017). Convergent validity is established when the AVE value is 0.50 or more. Tables 6 shows that the AVE value for reflective constructs range from 0.731 to 0.883, which indicates the measures within the construct are sharing a high proportion of variance (Hair et al., 2017). All the reflective indicators show item loadings above 0.70 (Tables 7), and at a significance level of 0.000. This suggests that the associated indicators share much in

common that is interpreted by the construct hence the indicator reliability is satisfactory (Hair et al., 2017).

Table 6. Cronbach's Alpha, Composite Reliability (CR) and Average Variance Extracted (AVE) of Reflective Constructs

Construct	Cronbach's Alpha	Composite Reliability	Average Variance Extracted (AVE)
Protection Motivation	0.934	0.958	0.883
Personalisation	0.923	0.951	0.867
Privacy Concern	0.929	0.942	0.731
Response Efficacy	0.861	0.915	0.782
Self-Efficacy	0.833	0.898	0.745
Fear	0.955	0.967	0.881
Perceived Severity	0.919	0.939	0.756
Perceived Vulnerability	0.933	0.952	0.833
Fear	0.950	0.964	0.869
Perceived Severity	0.927	0.945	0.775
Perceived Vulnerability	0.940	0.957	0.849

Table 7: Loadings and Cross-Loadings

	Protection Motivation	Privacy Concern	personalisation	Response Efficacy_	Self-Efficacy	Fear	Perceived Severity	Perceived Vulnerability	Maladaptive Reward	Cost
INTE1	0.948	-0.270	0.487	0.519	0.486	0.360	0.298	0.345	-0.364	-0.414
INTE2	0.960	-0.269	0.510	0.501	0.487	0.383	0.323	0.325	-0.331	-0.398
INTE3	0.910	-0.294	0.531	0.482	0.457	0.305	0.264	0.339	-0.280	-0.359
MPRI1	-0.284	0.923	-0.219	-0.093	-0.146	0.053	0.024	0.033	0.192	0.411
MPRI2	-0.286	0.929	-0.246	-0.204	-0.174	0.027	-0.003	-0.019	0.194	0.334
MPRI3	-0.248	0.935	-0.220	-0.150	-0.194	0.086	0.083	0.069	0.209	0.374
PERS1	0.477	-0.250	0.906	0.360	0.323	0.232	0.168	0.174	-0.209	-0.297
PERS2	0.519	-0.238	0.942	0.425	0.370	0.255	0.238	0.230	-0.200	-0.309
PERS3	0.515	-0.202	0.945	0.428	0.348	0.249	0.205	0.221	-0.196	-0.316
REEF1	0.444	-0.133	0.407	0.873	0.252	0.393	0.295	0.195	-0.202	-0.152
REEF2	0.457	-0.104	0.343	0.887	0.332	0.377	0.279	0.262	-0.157	-0.128
REEF3	0.510	-0.184	0.404	0.894	0.493	0.397	0.307	0.184	-0.145	-0.190
SEEF1	0.511	-0.147	0.386	0.378	0.868	0.165	0.149	0.280	-0.183	-0.211
SEEF2	0.432	-0.182	0.335	0.391	0.870	0.110	0.133	0.210	-0.151	-0.255
SEEF3	0.336	-0.144	0.211	0.280	0.853	0.060	0.021	0.140	-0.194	-0.237
Scenario #1 (Storm)										
V1_FEAR1	0.387	0.051	0.295	0.372	0.165	0.918	0.605	0.327	-0.106	-0.089
V1_FEAR2	0.355	0.044	0.267	0.411	0.166	0.931	0.556	0.265	-0.145	-0.073
V1_FEAR3	0.324	0.064	0.220	0.439	0.094	0.957	0.639	0.286	-0.113	-0.018
V1_FEAR4	0.331	0.058	0.209	0.430	0.095	0.947	0.645	0.246	-0.128	-0.041
V1_SEVR1	0.268	0.038	0.137	0.264	0.094	0.510	0.846	0.241	-0.023	0.024
V1_SEVR2	0.290	0.043	0.180	0.274	0.133	0.576	0.904	0.310	0.007	0.003
V1_SEVR3	0.236	-0.047	0.261	0.259	0.194	0.450	0.777	0.324	-0.038	-0.071

Table 7: Loadings and Cross-Loadings (Continued)

V1_SEVR4	0.285	0.038	0.187	0.333	0.083	0.639	0.912	0.306	-0.007	-0.022
V1_SEVR5	0.285	0.063	0.204	0.309	0.072	0.633	0.900	0.341	-0.001	0.010
V1_VULN1	0.326	0.045	0.180	0.231	0.194	0.309	0.367	0.904	-0.097	-0.004
V1_VULN2	0.314	0.024	0.230	0.207	0.241	0.272	0.301	0.898	-0.059	-0.002
V1_VULN3	0.326	0.000	0.225	0.205	0.246	0.250	0.286	0.918	-0.102	-0.083
V1_VULN4	0.341	0.029	0.189	0.233	0.251	0.261	0.319	0.932	-0.073	-0.009
Scenario #2 (Earthquake)										
V2_FEAR1	0.375	-0.001	0.395	0.292	0.134	0.914	0.542	0.353	-0.140	-0.182
V2_FEAR2	0.409	0.017	0.388	0.327	0.127	0.928	0.482	0.321	-0.117	-0.183
V2_FEAR3	0.383	0.020	0.364	0.357	0.130	0.954	0.495	0.298	-0.132	-0.173
V2_FEAR4	0.377	0.016	0.367	0.391	0.113	0.934	0.482	0.268	-0.142	-0.161
V2_SEVR1	0.279	-0.027	0.272	0.173	0.150	0.412	0.875	0.270	-0.021	-0.112
V2_SEVR2	0.324	-0.033	0.333	0.212	0.216	0.440	0.906	0.302	-0.027	-0.078
V2_SEVR3	0.305	-0.048	0.381	0.214	0.273	0.387	0.805	0.273	-0.126	-0.143
V2_SEVR4	0.411	-0.004	0.350	0.318	0.147	0.560	0.901	0.382	-0.075	-0.181
V2_SEVR5	0.369	-0.008	0.367	0.312	0.174	0.528	0.909	0.354	-0.067	-0.146
V2_VULN1	0.192	0.031	0.158	0.188	0.046	0.308	0.347	0.915	-0.047	-0.105
V2_VULN2	0.205	0.011	0.257	0.123	0.111	0.315	0.325	0.921	-0.104	-0.155
V2_VULN3	0.215	-0.026	0.228	0.127	0.081	0.309	0.332	0.932	-0.110	-0.098
V2_VULN4	0.237	-0.059	0.202	0.179	0.097	0.299	0.342	0.918	-0.096	-0.098

Table 7: Loadings and Cross-Loadings (Continued)

MALR1	-0.312	0.223	-0.189	-0.156	-0.207	-0.102	0.051	-0.070	0.898	0.415
MALR2	-0.228	0.088	-0.156	-0.081	-0.040	-0.140	-0.031	-0.120	0.657	0.269
MALR3	-0.225	0.114	-0.177	-0.157	-0.081	-0.174	-0.053	-0.118	0.649	0.215
MALR4	-0.213	0.188	-0.175	-0.119	-0.243	-0.116	-0.013	-0.089	0.614	0.325
MALR5	-0.282	0.178	-0.154	-0.143	-0.171	-0.118	0.001	-0.095	0.812	0.407
MALR6	-0.260	0.124	-0.197	-0.161	-0.112	-0.166	-0.084	-0.118	0.750	0.209
COST1	-0.113	0.182	-0.091	0.024	-0.124	0.138	0.163	-0.027	0.103	0.273
COST2	-0.362	0.363	-0.287	-0.143	-0.297	-0.051	-0.044	-0.028	0.380	0.870
COST3	-0.402	0.415	-0.332	-0.167	-0.245	-0.058	-0.012	-0.005	0.375	0.966
COST4	-0.103	0.301	-0.230	-0.059	-0.229	0.028	0.123	0.085	0.289	0.249
COST5	-0.323	0.372	-0.324	-0.145	-0.344	0.029	0.118	-0.026	0.358	0.776
COST6	-0.251	0.346	-0.235	-0.105	-0.231	0.025	0.139	0.014	0.264	0.605

Discriminant validity describes the extent to which a construct is truly distinct from other constructs by empirical standards for reflective measurements (Hair et al., 2017). Examining the Fornell-Lacker Criterion and cross-loadings are two main approaches that were used to assess the discriminant validity (Hair et al., 2017). The first approach compares the square root of the AVE value with the latent variable correlations ((Hair et al., 2017). As shown in Table 8, for each reflective construct, the square root of the AVE value is greater than its strongest correlation with any other construct. Also, as expected, for the indicators of reflective constructs, their loadings on their associated constructs are greater than their cross-loadings on any other constructs (Hair et al., 2017). Overall, the results from assessing the Fornell-Lacker Criterion (Table 8) and cross-loadings (Table 7) provide evidence for satisfactory discriminant validity of the measurement model. Altogether the results indicate that our measurement model has sufficient reliability and validity necessary to proceed with the evaluation of structural model and hypotheses.

Table 8: Fornell-Lacker Criterion

Construct	1	2	3	4	5	6	7	8
1. Protection Motivation	0.940							
2. Personalisation	0.541	0.931						
3. Privacy Concern	-0.266	-0.206	0.855					
4. Response Efficacy	0.533	0.435	-0.158	0.885				
5. Self-Efficacy	0.507	0.373	-0.163	0.413	0.863			
Scenario #1 (Storm)								
6. Fear	0.372	0.264	0.064	0.440	0.138	0.939		
7. Perceived Severity	0.315	0.220	0.048	0.333	0.127	0.653	0.870	
8. Perceived Vulnerability	0.358	0.225	0.053	0.240	0.254	0.300	0.350	0.913
Scenario #2 (Earthquake)								
6. Fear	0.414	0.407	0.036	0.365	0.135	0.932		
7. Perceived Severity	0.390	0.388	-0.011	0.287	0.213	0.538	0.880	
8. Perceived Vulnerability	0.231	0.230	0.010	0.167	0.091	0.334	0.365	0.921

5.3.2 Formative (Composite) Constructs

In this study, response cost and maladaptive rewards were modeled as formative constructs. Response cost had 6 indicators and maladaptive rewards had 6 indicators (See Appendix C). To assess the formative models, two criteria were examined – collinearity and indicator weights and loadings.

Collinearity assesses the extent to which two formative indicators are correlated; when formative indicators are highly correlated, this can have an impact on the assessment of the weights and statistical significance (Hair, et al., 2017). To assess collinearity, variance inflation factor (VIF) can be examined, where a VIF of 5 and higher indicates a potential collinearity problem (Hair et al., 2017). If collinearity is high, Hair et al (2017) suggest removing one of the corresponding variables. The initial results showed the VIF exceed 5.0 for MALR3 and MALR6 with 6.826 and 7.438 respectively. To address, each item was removed (one at a time) and the measurement model was reassessed. The results showed that removing MALR3 (effort) had the least impact; MALR3 was therefore removed from the measurement model.

The second criterion (indicator weights and loadings) assesses the relevance of the indicator to the formative construct (Hair et al., 2017). Indicator weights indicate the relative contribution (or importance) of the indicator to the construct, while the loadings signal the absolute contribution of the indicator to the construct irrespective of the other indicators. Both assessments are important for even if an indicator is relatively low in its contribution to a construct, its absolute importance to the construct may be significant (Hair et al., 2017). If both are below acceptable levels (0.50), then the theoretical relevance and potential overlap with other items should be examined to decide if the item should be kept or removed (Hair et al., 2017).

The results (Table 9) showed that for maladaptive rewards (after removing MALR3), the weights ranged from -0.149 to 0.747 with MALR1 (0.747) and MALR6 (0.638), being significant (at $p \leq 0.05$). For response cost, the indicator weights ranged from -0.208 to 0.722 with COST3 being the only indicator with a significant weight (0.722, $p \leq 0.01$). All other items for both constructs were nonsignificant and below 0.50, suggesting that only COST3, MALR1 and MALR6 were relatively important compared with other indicators in forming their respective constructs. Five items for response cost and three items for maladaptive rewards therefore had nonsignificant weights. The

absolute importance (i.e. loadings) of the indicators was then examined. The results (Table 9) showed the loadings for maladaptive rewards ranged from 0.624 to 0.913 with no indicator below 0.50; all items were therefore retained. For response cost, the loadings ranged from 0.249 to 0.966, with COST1 (0.272) and COST4 (0.249) falling below 0.50. Since COST1 and COST4 fell below 0.50, the theoretical relevance and potential overlap with other items was then examined.

For response cost, prior research suggests that an ideal way to measure response cost is to include monetary cost (e.g. COST1) and non-monetary cost (e.g. COST2, COST3) that cover functional (e.g. COST4, COST5) aspects and uncertainty aspects (e.g. COST6). The items were adapted from previous research which passed the validity check based on the prior studies (Woon et al., 2005), and are in line with the recommended approach for measuring response cost. Each indicator was further informed by knowledge of the study context. Altogether these were considered relevant from a theoretical and content perspective. As such, all six indicators were retained for further evaluation (Bockarjova and Steg, 2014; Hair et al., 2017). However, it is recommended that future research revisits and improves the measures.

Table 9: Loadings, Weights, and Variance Inflation Factor (VIF) of Formative Constructs

	Indicator Weights		Indicator Loadings		
	weights	p-value	loadings	p-value	VIF
COST1	-0.109	0.489	0.272	0.034	1.471
COST2	0.134	0.598	0.870	0.000	3.647
COST3	0.722	0.002	0.966	0.000	3.592
COST4	-0.208	0.248	0.249	0.122	1.443
COST5	0.237	0.322	0.776	0.000	3.200
COST6	0.137	0.533	0.605	0.000	2.446
MALR1	0.747	0.011	0.913	0.000	3.455
MALR2	-0.257	0.409	0.667	0.000	3.766
MALR4	-0.192	0.387	0.624	0.000	2.198
MALR5	0.149	0.635	0.825	0.000	4.092
MALR6	0.638	0.029	0.762	0.000	3.496

5.4 Inner (Structural) Model Assessment

The assessment of the structural model focuses on evaluating the significance and relevance of the relationships in the structural model (Hair et al., 2017). The coefficient of determination (R^2 value) is used to present the model's predictive power. R^2 is the squared correlation between actual and predicted values, which ranges from 1 to 0 (Hair et al., 2017). Threshold values of 0.25, 0.5, and 0.75 are used to describe a weak, moderate and strong coefficient of determination (Hair et al., 2017; Wong, 2016). In general, the higher the value of R^2, the better the model fits the data. From the PLS path model estimation diagram (see Figure 6), the overall R^2 (i.e. variance explained) is found to be a moderate one (Scenario #1: $R^2 = 0.56$, Scenario #2: $R^2= 0.55$).

To evaluate the path coefficients between individual constructs, t-values, p-values and bootstrapping path coefficients are evaluated using the results from the PLS bootstrapping algorithm; 5000 bootstrap samples were used for running the bootstrapping procedure. The results are also shown in Figure 6, which include the path coefficients (β), significance levels, and the variance explained (R^2) in each endogenous variable.

Next, we report the results of the model tests. Scenario #1 and Scenario #2 are assessed using separate models in order to understand the relative impact of a context-specific evaluation of fear appeal in relation to the threat appraisal, the coping appraisal and protection motivation.

5.4.1 Result of Structural Model Test

Table10 shows the estimated path coefficients for both scenarios. The combined factors of threat appraisal, coping appraisal and the privacy and personalisation trade-off accounted for approximately 0.564 of the variance explained for protection motivation in Scenario #1, and approximately 0.551 in Scenario #2. For fear appeal, 0.432 of the variance is explained for Scenario #1, and 0.311 is explained for Scenario #2. The results of the structural model tests are shown in Figure 6 and are further discussed below.

Table 10: Model Tests for Scenario #1 and #2

	R^2	T Statistics	P Values
Scenario #1 (Storm)			
Protection Motivation	0.564	13.700	0.000
Fear	0.432	8.834	0.000
Scenario #2 (Earthquake)			
Protection Motivation	0.551	13.297	0.000
Fear	0.311	5.716	0.000

Altogether the results for fear appeal provided consistent support for perceived severity in relation to fear (H2a), but the results were inconsistent for the other relationships, and provided partial support for the hypotheses. Scenario #1(Storm) showed that of the five hypotheses related to fear appeal, only the relationships between perceived severity and fear (H2a), and between perceived vulnerability and protection motivation (H1b) were supported. For Scenario #2 (Earthquake), all the relationships were significant (i.e. H1a, H2a, H2b, H3) except for the relationship between perceived vulnerability and protection motivation (H1b).

The results for Scenario #1 (Storm) revealed that for fear appeal, perceived severity of the emergency was significant in determining fear (H2a: $\beta=0.624$, $p\leq0.001$). However, there was no significant relationship found between perceived severity and protection motivation (H1a: $\beta=0.063$, $p>0.10$). That is to say, while perceived seriousness of the storm was significantly related to the level of fear such that greater seriousness was associated with greater fear, it did not have a direct and significant impact on protection motivation to disclose personal information. Hence, H2a was supported for Scenario #1 while H1a was not. On the other hand, perceived vulnerability showed no significant association with fear (H2b: $\beta=0.082$, $p>0.1$), but it was significant in relation to protection motivation (H1b: $\beta=0.149$, $p\leq0.05$). Hence, H1b was supported whereas H2b was not. Fear was also found to be non-significant in relation to protection motivation (H3: $\beta=0.100$, $p>0.10$), and therefore, H3 was not supported for Scenario #1.

For Scenario #2 (Earthquake), perceived severity (H2a: $\beta=0.48$, $p\leq0.001$) and perceived vulnerability (H2b: $\beta=0.159$, $p\leq0.05$) were both found to significantly influence fear, and fear in turn, was shown to be significantly related to protection motivation. Hypotheses H2a, H2b and H3 were therefore supported for Scenario #2. Perceived severity (H1a: $\beta=0.104$, $p\leq0.1$) was also shown to be a predictor of protection

motivation, however no evidence was found to support the relationship between perceived vulnerability (H1b: β=0.024, p>0.1) and protection motivation. Thus, H1a is supported for Scenario #2 whereas H1b is not.

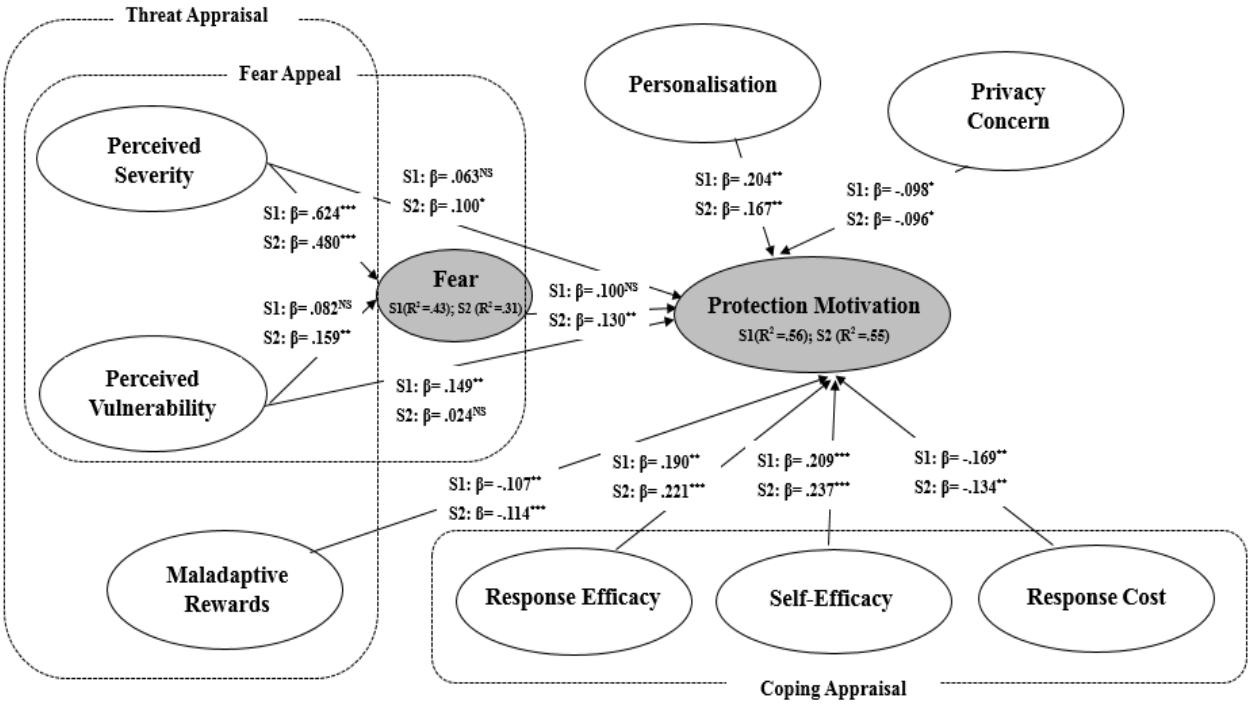
Maladaptive rewards (Scenario #1: β= -0.107, p≤0.05; Scenario #2: β = -0.114, p≤0.05) had a significant but inverse impact on protection motivation. Hence, H4 was supported.

For the coping appraisal, the antecedent variables were significant in respect of protection motivation, that is, response efficacy (Scenario #1: β=0.190, p≤0.05; Scenario #2: β=0.221, p≤0.001), self-efficacy (Scenario #1: β=0.209, p≤0.001; Scenario #2: β=0.237, p≤0.001) and response cost (Scenario #1: β = -0.169, p≤0.05; Scenario #2: β= -0.134, p≤0.05). Hence, H5, H6 and H7 were supported.

Turning to the personalisation-privacy concern trade-off, the results showed that the impact of both personalisation (Scenario #1: β =0.204, p≤0.05; Scenario #2: β =0.167, p≤0.05) and privacy concern (Scenario #1: β = -0.098, p≤0.10; Scenario #1: β = -0.096, p≤0.1) were significant in relation to protection motivation. Therefore, H8 and H9 were supported. The results showed a positive relationship between the perceived level of personalisation of PMEAS and behavioral intention, such that personalisation would act as a motivator to disclose personal information. In contrast and as expected, privacy concern regarding information disclosure was inversely related to behavioral intention. With personalisation having a stronger positive impact on protection motivation, and privacy concern having a lower negative impact, it is expected that the negative consequences of privacy concerns would be overweighed by the perceived benefits of personalised services from using PMEAS.

The control variables that is, gender, age, education, geographical region, and personal innovativeness, were tested one by one in the structural models. The results showed that none of the control variables was significant in explaining the differences among subjects in relation to protection motivation.

Figure 6: Test Results of the Research Model



Significance Level: ***p≤0.001; ** p≤0.05; * p≤0.10

S1: Scenario #1(Storm); S2: Scenario #2 (Earthquake)

Table 11: Test of Hypotheses for Scenario #1 and #2

Scenario	**Scenario #1**			**Scenario #2**		
Hypothesis	**Path Coefficients**	**P-Value**	**Supported**	**Path Coefficients**	**P-Value**	**Supported**
H1a: Perceived Severity of an emergency threat is positively related to Protection Motivation to use a PMEAS.	0.063	0.313	No	0.100	0.104	Yes*
H1b: Perceived Vulnerability of an emergency threat is positively related to Protection Motivation to use a PMEAS.	0.149	0.002	Yes**	0.024	0.654	No
H2a: Perceived Severity of emergency threat is positively related to Fear.	0.624	0.000	Yes***	0.480	0.000	Yes***
H2b: Perceived Vulnerability of emergency threat is positively related to Fear.	0.082	0.140	No	0.159	0.019	Yes**
H3: Fear of an emergency is positively related to Protection Motivation to use a PMEAS.	0.100	0.135	No	0.130	0.023	Yes**
H4: Maladaptive Rewards is inversely related to Protection Motivation to use a PMEAS.	-0.107	0.048	Yes**	-0.114	0.027	Yes**
H5: Response Efficacy is positively related to Protection Motivation to use a PMEAS.	0.190	0.006	Yes**	0.221	0.001	Yes***
H6: Self-Efficacy is positively related to Protection Motivation to use a PMEAS.	0.209	0.000	Yes***	0.237	0.000	Yes***
H7: Response Cost is inversely related to Protection Motivation to use a PMEAS.	-0.169	0.005	Yes**	-0.134	0.022	Yes**
H8: Privacy Concern is inversely related to the willingness to disclose personal information to use a PMEAS.	-0.098	0.066	Yes*	-0.096	0.072	Yes*
H9: Personalisation is positively related to the willingness to disclose personal information to use a PMEAS.	0.204	0.002	Yes**	0.167	0.017	Yes**

5.5 Chapter Summary

This chapter presents the model evaluation results for both the measurement (outer) model and the structural (inner) model. The assessments of the reflective and formative constructs revealed sufficient validity and reliability of the model constructs and indicators. On the other hand, the results also showed the structural model can explain 0.311 and 0.432 of the variance observed for fear appeal and, 0.551 and 0.564 of the variance observed for protection motivation (for Scenarios #1 and #2 respectively).

Table 12 summarizes the results of hypotheses testing. It shows a satisfactory result for hypotheses testing. For Scenario #1 (Storm), most of the hypotheses are supported apart from three hypotheses related to fear appeal and the threat appraisal (H1a, H2b and H3). For Scenario #2 (Earthquake), all the hypotheses are supported except H1b. The differences in influence are attributed to the differences in the fear appeal contexts (i.e. Scenario #1 – Storm versus Scenario #2 – Earthquake). However, these did not have a significant impact on the overall explanatory power of the model, beyond the small differences in the relative impact of the antecedents on protection motivation (due to changes in fear appeal), as signaled by the path coefficients. Hence, it can be concluded that although individuals' risk perceptions differ in relation to fear appeal and how it impacts protection motivation, the PMT together with personalisation and privacy concern is still an effective model for examining an individual's willingness to disclose personal information to PMEAS. In addition, results showed that a high level of personalisation provided by PMEAS can be strong enough to motivate an individual to disclose their personal information, such that privacy concerns though negative, has a lesser effect on personal information disclosure.

Table 12: Results of Hypotheses Testing

Hypotheses	**Results**	
	Scenario #1	**Scenario #2**
H1a: Perceived Severity of an emergency threat is positively related to Protection Motivation to use a PMEAS.	Not Supported	Supported
H1b: Perceived Vulnerability of an emergency threat is positively related to Protection Motivation to use a PMEAS.	Supported	Not Supported
H2a: Perceived Severity of emergency threat is positively related to Fear.	Supported	Supported
H2b: Perceived Vulnerability of emergency threat is positively related to Fear.	Not Supported	Supported
H3: Fear of an emergency is positively related to Protection Motivation to use a PMEAS.	Not Supported	Supported
H4: Maladaptive Rewards is inversely related to Protection Motivation to use a PMEAS.	Supported	Supported
H5: Response Efficacy is positively related to Protection Motivation to use a PMEAS.	Supported	Supported
H6: Self-Efficacy is positively related to Protection Motivation to use a PMEAS.	Supported	Supported
H7: Response Cost is inversely related to Protection Motivation to use a PMEAS.	Supported	Supported
H8: Privacy Concern is inversely related to the willingness to disclose personal information to use a PMEAS.	Supported	Supported
H9: Personalisation is positively related to the willingness to disclose personal information to use a PMEAS.	Supported	Supported

6. Discussion

6.1 Discussion of Results

Today, the world is increasingly subject to emergency threats which are potentially harmful to individual's physical and mental well-being whether these arise from natural disasters, such as earthquakes and flooding, or from human action such as terror attacks, war, or accidents. In response, many countries have in place Emergency Management Programs (Nazarov, 2011; NASA, 2013). Prior research provides a record of evidence that actions taken to influence and manage behavior would help to reduce the potential damage to an individual's well-being from those threats (Bockarjova and Steg, 2014; Mulilis and Lippa, 1990; Wolf et al., 1986). Protection Motivation Theory (PMT) lends itself as a useful theoretical framework to better understand individuals' attitude and behavioral intention arising from their cognitive evaluation of potential threats and coping responses.

In this research, Protection Motivation Theory (PMT) is applied, with the incorporation of personalisation and privacy trade-off, to understand an individual's intention to disclose personal information in the context of PMEAS that would provide information that can help them respond appropriately and take actions to reduce the impacts of the threat. Based on the theoretical foundation, three research questions are examined:

(1) What factors impact an individual's willingness to disclose personal information in the context of using a PMEAS?
(2) What impact does the trade-off between privacy concern and personalisation have on an individual's willingness to disclose personal information in the context of using a PMEAS?
(3) What impact does risk perception have on an individual's willingness to disclose personal information in the context of using a PMEAS?

The model test results demonstrate a moderate predictive power of our model in explaining Protection Motivation in terms of behavioral intention to disclose personal information to use a PMEAS. The current study shows that in the context of PMEAS, the effects of threat appraisal, coping appraisal and the privacy-personalisation trade-off are significant in determining an individual's willingness to disclose personal

information. Hence, the testing of the hypotheses revealed satisfactory and interesting outcomes that contribute to addressing the research questions.

Research Question 1: What factors impact an individual's willingness to disclose personal information in the context of using a PMEAS?

For the first research question the results show that constructs including response efficacy, self-efficacy, response cost, and maladaptive rewards from the PMT, and personalisation and privacy concern are key factors that impact an individual's willingness to disclose personal information in the context of using a PMEAS. The results further show that fear appeal is highly context-sensitive such that both perceived severity and perceived vulnerability were significantly related to fear for an earthquake emergency, while only the relationship between perceived vulnerability and fear was supported for the storm emergency.

In line with numerous findings in the health-threat literature applying PMT (Cates et al., 2010; Leventhal, 1970; Rogers, 1975; Rippetoe and Rogers, 1987), our study showed that the perception of a threat reinforces behavioral intentions to adopt the recommended response. On the other hand, fear acted as a driver to alter or mediate the impact of the threat perceptions on behavioral intention (i.e. willingness to disclose personal information in order to use PMEAS).

Perceived severity of an emergency threat was positively related to fear for both emergency scenarios. However, hypothesis H1a "perceived severity of an emergency threat is positively related to protection motivation to use a PMEAS" was significant only for Scenario #2 (Earthquake) but not in Scenario #1 (Storm). Similarly, perceived vulnerability was shown to be significant in relation to fear for Scenario #2 but for Scenario #1. Hence, the findings suggest that for fear appeal, perceived severity and perceived vulnerability are context-sensitive such that their impact on protection motivation (i.e. to disclose personal information) differs for different contexts. One of the possible reasons for the different outcome might be that respondents were more aware and concerned about an earthquake - in the earthquake scenario, both perceived severity and perceived vulnerability were significant in relation to fear, and fear and severity were significant in relation to protection motivation. This may because New Zealand has been impacted by four severe earthquakes in the past 7 years, which had

widespread effects across Christchurch, Wellington, and Kaikoura regions. For example, Christchurch is still recovering from the 2011 event with major demolition and building projects still underway. On the other hand, floods may occur across all regions, and have done so especially in the north island, and on the upper south island and west coast. While persons' vulnerability to storms influenced their motivation to protect themselves by using PMEAS, perceived severity did not have a similar impact on protection motivation, except through its impact on fear.

The inconsistent performance of fear appeal on protection motivation is in line with previous research. On the one hand, some studies demonstrated a significant relationship such as Menard et al.'s study (2014), in which both perceived severity and vulnerability of losing data had strong impacts on participants' intention to back up data on the cloud. Lee and Larsen (2009) also found perceived severity was the most influential variable encouraging CEOs of Small Medium Business (SMB) to adopt anti-malware software. On the other hand, other studies using PMT yielded quite different outcomes (Murgraff et al., 1999; Meso et al., 2013). For example, in a comparison study (Kim et al., 2012) of pro-environment behaviour between Korean and American students, perceived severity of negative environmental impacts was significant for attitude change and behavioral intention while perceived vulnerability was not. Prior research (Plotnikoff and Higginbotham, 1998) has further suggested that threat appraisal is a problematic construct in PMT study because of the difficulty in manipulating perceptions within a general population. As a result, studies have shown perceived severity to be both context-specific and individual-specific in determining behavioral intention and actual behaviour (Ifinedo, 2012; Lee, 2011; Pechmann et al., 2003).

Turning to the main model, the results showed a consistent association between coping appraisal and protection motivation, which is in line with Milne et al.'s (2000) findings of their meta-analysis regarding PMT, where the components of coping appraisal yielded stronger impacts in determining the behavioral intention than the components of threat appraisal. Prior research also suggests that self-efficacy is a strong predictor in PMT (Johnston and Warkentin, 2010; Plotnikoff and Higginbotham, 1998; Plotnikoff et al., 2009). Similarly, in our study, self-efficacy was also a strong facilitator of participant willingness to disclose information to PMEAS as they are confident in their capabilities to adopt, use and maintain a PMEAS. The significant effect of response efficacy on information disclosure intention also indicates that when participants

perceive high effectiveness in adopting the recommend protective actions from PMEAS in the case of an emergency, they are more motivated to disclose personal information for PMEAS use. Consist with prior research (Arthur and Quester, 2004; Ruthig, 2016), there was also a strong negative impact for response cost on protection motivation indicateing that the costs associated with the adoption, operation and maintenance of PMEAS will reduce participants' intention to disclose personal information to use these services.

None of the control variables was found to be significant in relation to protection motivation in this study. This result was consistent with prior work (Li et al., 2011) that investigated consumers' decision to disclose personal information to unfamiliar online vendors. One of the possible reasons is that our participants were all mobile users. 84% were already using some sort of Location-Based Services (LBS), indicating that they were already experienced with disclosing their personal information to online service providers.

Finally, when taken altogether our research demonstrated that the two cognitive mediating processes in PMT (threat appraisal and coping appraisal) were both significant in predicting individual's information disclosure intention in PMEAS though fear appeal operated differently in the model due to differences in the context.

Research Question 2: What impact does the trade-off between privacy concern and personalisation have on an individual's willingness to disclose personal information in the context of using a PMEAS?

To address research question 2, in this study we examined the impacts of personalisation and privacy concern on protection motivation (i.e. willingness to disclose personal information to use PMEAS). In our study, both privacy concern and personalisation have strong impacts on protection motivation in relation to disclosing personal information to a PMEAS provider.

Traditional privacy research indicates that privacy concerns is a "balancing act" (Altman, 1975; Petronio, 2012), that is, individuals need to decide what information to disclose and to whom it should be disclosed. At the same time, recent research (Christofides et al., 2009) in information disclosure also suggests that despite the

existence of privacy concerns, individuals are still willing to disclose a great deal of personal information (e.g. pictures., date of birth and email address on social media) due to the perceived benefits of such information disclosure. The findings of this research demonstrate that personalisation has a stronger impact in relation to protection motivation (i.e. intention to disclose personal information to PMEAS) than privacy concern. This suggests that the perceived benefit that would be derived from personalised services would be a stronger motivator for them to disclose personal information in exchange for the customized service than concerns about privacy in relation to not disclosing personal information.

Research Question 3: What impact does risk perception have on an individual's willingness to disclose personal information in the context of using a PMEAS?

According to previous research (Rogers, 1975; Rogers, 1983; Wolf et al., 1986), the effects of a fear-arousing communication (fear appeal) on behavioral intentions would be mediated indirectly by changes in predictor variables such as perceived severity, perceived vulnerability and fear.

As discussed in Chapter 2, while enhancing fear appeal may lead to people following the recommended adaptive actions in a risk-mitigating context (Taylor and May, 1996), examining the individual impact of perceived severity and vulnerability on protection motivation may yield different outcomes. For example, prior studies suggest perceived vulnerability is a strong predictor of intention only in certain contexts (Ifinedo, 2012; Pechmann et al., 2003).

As the result of a t-test shows in our study, participants had a general tendency to perceive the earthquake scenario to be more severe and their susceptibility to be higher than the storm scenario, indicating that in general they felt they were more susceptible to, and so were more fearful of an earthquake emergency. In other words, the prospect of being impacted by a severe earthquake aroused more fear than the prospect of being impacted by a storm. The results showed that fear aroused by the earthquake scenario acted as a stronger and significant motivator of protection motivation, while the fear perceptions associated with the storm emergency did not have a significant impact on protection motivation. While perceived severity was also a consistent predictor of fear for both scenarios, and had a significant direct impact on protection motivation,

perceived vulnerability was impactful only in relation to fear for storm scenario (but not for earthquake scenario). Consistent with prior research, these findings provide evidence to suggest that differences between risk perceptions can have significantly different impacts on behavioral intention (Taylor and May, 1996; Ifinedo, 2012).

6.2 Summary

This study extends protection motivation theory to incorporate personalisation and privacy concern to explain protection motivation towards using a PMEAS, which is conceptualized in this study as an individual's willingness to disclose personal information in order to use a PMEAS. Using survey data from 261 mobile users in New Zealand, the proposed model was empirically tested using SmartPLS (version 3.2.6).

The research findings suggest that coping appraisal acts as the strongest predictor in the model; response efficacy, self-efficacy and response cost were all significant in relation to protection motivation. For the privacy-personalisation trade-off, both privacy concern and personalisation had strong impacts on the protection motivation to disclose personal information.

Threat appraisal and fear appeal, on the other hand, revealed some differences compared with previous research (Meso et al., 2013; Siponen et al., 2006). While maladaptive rewards had a strong effect on protection motivation, the relationship between perceived severity, perceived vulnerability, fear and protection motivation were shown to be dependent on the context of the emergencies due to the fear appeal, so had different impacts in relation to both fear and protection motivation for the same respondent. In this study, perceived severity was significant in relation to fear in both scenarios. The relationship between perceived vulnerability and protection motivation was significant in the storm scenario but not in the earthquake scenario. In contrast, the remaining relationships in fear appeal (between perceived severity and protection motivation, fear and protection motivation, and perceived vulnerability and fear) were found to be significant in the earthquake scenario but not in the storm scenario.

In summary, our study provides good empirical evidence that PMT is a valuable tool for understanding and explaining individual's willingness to disclose personal information to PMEAS. Our research also demonstrated that PMT can be extended to

contexts other than health-related issues and include other variables to explain attitude and behavior (such as privacy concern and personalisation in this study). The findings further highlight the context-sensitive nature of the fear-appeal aspect of the PMT in emergency research.

7. Conclusion

The following sections first highlight the research contribute from both theoretical and practical perspectives. Then limitations of this study are discussed, followed by directions for future research.

7.1 Research Contribution

This research makes several contributions to the literature and to practice. For theory, this study extends the PMT model by combining the personalisation and privacy trade-off with PMT concepts in the context of PMEAS use. Empirical evidence has been provided to support the model tests. For practice, several implications are discussed based on the research findings that aim to inform PMEAS designers, implementers and government agencies. The findings are expected to provide these audiences with a better understanding of potential users' perceptions of PMEAS and the factors that would influence user's intention to use a PMEAS by disclosing personal information. These contributions are further discussed in the following sections.

7.1.1 Contribution to Theory

Previous literature in emergency alert systems was mainly conducted from design and implementation perspectives (Báez et al., 2017; Hunter et al., 2007; Palen et al., 2010; Tupler and Mock, 2007). Very few empirical studies have been done to address factors that influence potential user's intention of system adoption. Moreover, no empirical study using quantitative methods has been done in the specific context of PMEAS. Hence, our study contributes to the exiting literature by bridging a gap in emergency notification research and enhancing the understanding of context-specific factors (e.g. perceived severity, perceived vulnerability and fear of emergency) that influence people's behavioral intention on information disclosure.

Protection Motivation Theory (PMT) has been widely used to explore individual's protection motivation (i.e. intention to engage in protective response) in health-related topics. However, it has not been applied and tested in the context of emergency notification. As an initial attempt to apply the PMT model to the context of PMEAS,

this study has confirmed that PMT is useful for examining attitude and behaviour in the emergency context. More importantly, this research suggests that the PMT model can be extended to include the personalisation and privacy trade-off in evaluating an individual's intention to disclose personal information to PMEAS.

Finally, two emergency scenarios (storm and earthquake) were used to focus the participants' responses in this study. Although the two scenarios had similar overall impacts on behavioral intention, individual's threat appraisal of each emergency scenario was shown to differ. Hence, our research contributes to theory by demonstrating that the manipulation of fear appeal would create variances across individual's risk perceptions about the emergency which is in line with previous studies using PMT (Boss et al., 2015; Milne et al., 2000). Furthermore, we measured the perceptions of both emergency scenarios for the same respondent (i.e. participants were asked questions about Scenario #1 and Scenario #2). This differs from prior studies that often apply two different scenarios into different groups (i.e. participants were asked questions about either scenario #1 or scenario #2; e.g. Boss et al., 2015; Malhotra et al., 2004). Instead, our findings show that even the same person may have different risk perceptions due to changes in fear assessment.

7.1.2 Implications for Practice

This study provides some important implications for PMEAS designers, service providers and government agencies. First, the results of this study indicate that using information about an emergency that is familiar to the targeted audience will have a more successful fear-appeal and better motivate the corresponding actions. Prior research in information system adoption (Yang and Lee, 2016) indicate that no matter how elaborately the security policy is that has been established, without users' sufficient awareness of the severity of the threats, their satisfaction with the system, as well as their self-efficacy will decrease. In our study, the two emergency scenarios were designed specifically for the research purpose of focusing on situations that are familiar to people in New Zealand. Factors like perceived severity and susceptibility were fairly relatable to many, given the recent disasters. However, this may not always be the case. To address this lack of exposure and improve peoples' readiness for an emergency, in New Zealand there is currently a promotional campaign to raise awareness of fire emergencies and actions that should be taken. To support the campaign, a fire service

app using virtual reality is being rolled out. By providing a virtual experience of escaping a house (based on the user's setting using any real address in New Zealand or identifying the structure of the house), users are encouraged to explore different exits and interact with items and obstacles they encounter (Junn, 2017). The "frightening" experience being set in a place that is familiar to the people is expected to shift people's behavior to take protective actions to pre-empt a real fire emergency in the future. Similarly, it is recommended that the design and implementation of PMEAS present information that is understandable to the audience. The purpose is to help people recognize the severity of the emergency using fear-appeal communication, and encourage appropriate actions. In the case of PMEAS, the first step towards protection is to sign-up and provide (disclose) the information so that communication can be better tailor to the receivers' situation.

Second, current PMEAS focus on targeting a wide audience. For example, "Hazards" in New Zealand is a PMEAS that attempts to notify all people nationwide of an emegrncy. "RapidNotify" provides a similar notification service for people across North America (Rapid Notify, 2017). However, PMEAS that attempt to notify persons in a large geographical region may result in issues such as a mismatch between emergency alerts and users' needs and expectations. Reviews (on the App Store) from users of "Hazards" indicate that while some persons are expecting notifications about storms and heavy rains since they are living by the sea (as this may result in floods that cause harm and damage), others are not equally worried about it since where they are living is less vulnerable to this type of disaster. Similar to real-life situations, our research suggests that individuals do not see themselves as equally vulnerable to the same emergencies, so will have different perceptions of a threat which in turn would impact their protection motivation differently. The results indicate people who feel more vulnerable to an emergency will be more willing to use a PMEAS by disclosing personal information. Hence, PMEAS designers should consider targeting potential users who are more vulnerable to certain emergencies, rather than trying to notify everyone with the same information.

Finally, our findings suggest that privacy concerns about personal information is not absolute in the use of PMEAS; rather, it can be traded off against personalised emergency alerts. This leaves plenty of opportunities for PMEAS providers and government agencies to design and implement services that are tailored to users' preferences. At the same time, they should consider incorporating more privacy-

enhancing mechanisms. Notably, privacy-enhancing mechanisms are well-developed and have been adopted by some emerging location-based services (Sun et al., 2009). Policy-based techniques are one example, which in this research context refers to the use of privacy policies for PMEAS that define restrictions that regulate the release of personal information (e.g. location, name, home address, etc.) to third parties (Ardagna et al., 2008). This can help avoid misuse of personal information and assure users that their information will be protected.

7.2 Limitations of the research

Notwithstanding the contributions to knowledge, there are limitations that need to be addressed in this study. McGrath (1981) described the research strategy domain as a "three-horned dilemma", which argues that empirical studies are subjected to inherent limitations in: (a) generalizability with respect to populations; (b) precision in control and measurement of behavioral variables; or (c) realism of the context in which participants are observed. It is no doubt that the interpretation and application of the research findings in this study would be subject to similar limitations.

More specifically, since the sample in this study focused on mobile users in New Zealand, this sample may not be representative of populations outside New Zealand. As a result, while the findings are relevant to the population represented by the sample, it may not be generalizable to the wider population. In particular, the vignettes were designed to focus on contexts that were familiar to New Zealand respondents. To improve generalizability, it is recommended that future studies test the model with other context-specific scenarios such as bushfires in Australia, and tornados in the USA.

Second, this study used a one-shot survey with vignettes to represent hypothetical context, responses to the "hypothetical situation" may not exactly reflect the participants' behaviour in real-life situations. In addition, the selection of behavioral measures focused on behavioral intention rather than observations of actual behavior. This is mainly because PMEAS are currently not accessible to most of the participants, so that actual behaviour would not be assessed in this study. Nevertheless, it is worth mentioning that more PMEAS are under development in New Zealand for future use, particularly following the severe damage caused by the magnitude 7.8 Kaikoura earthquake (Stuff, 2017). Future research can therefore be conducted using longitudinal

study to collect data for both intention and actual behavior by testing those newly developed PMEAS. Similarly, studies can also be conducted in contexts such as Australia and Japan which have well-established PMEAS.

Finally, the results showed that some of the measures for response cost and maladaptive rewards were not important for the current context. For response cost, the results showed no significance for two items (i.e. COST1 assessing data usage and COST4 assessing the impact of PMEAS on other applications), that is, the item weights were nonsignificant and loadings were below 0.50. Although one option is to drop such items, it was recommended that the theoretical importance of the items to the construct is considered (Hair et al. 2017). Given the selection of items was informed by the prior literature (Boss et al., 2015; Woon et al., 2005) and knowledge of costs associated with using PMEAS (e.g. data usage, money, etc.) in the study context, both items were retained. It is however recommended that future work reassesses these items in contexts where there may be more variability in terms of people's perceptions of the cost of using PMEAS (such as the cost of data usage and impact on other applications).

For maladaptive rewards, the results also showed a high level collinearity among two items - MAL3 (Not using a personalised MEAS would save me effort) and MAL6 (Not using a personalised MEAS would avoid unnecessary disruption). To address this problem, both indicators were assessed, and MAL3 was removed as it was shown to have the least impact on the content of construct. Also from a theoretical perspective it can be argued that items measuring costs such as time and money were sufficient for capturing the effect of the 'effort' needed in using a PMEAS). Nonetheless, although the choice of indicators was informed by prior research (Myyry et al., 2009) and knowledge of the study context, it is suggested that future research re-examines this construct more closely.

7.3 Directions for future research

In this study, fear manipulation using short vignettes describing two emergency situations revealed significant differences in participant's threat perceptions, but similarity in terms of the behavioral intention. However prior research suggests that the description of a threat alone does not cue differences in coping responses (Rippetoe and Rogers, 1987). Prior study further suggests a fear-arousing message containing not only

threat information but also efficacy-enhancing message would be more persuasive to shift an individual's behaviour (Kim et al., 2012) Also, the type of coping information received has a differential effect on the behavioral intention (Rippetoe and Rogers, 1987). Hence, it is recommended that future research in PMEAS using PMT includes information about the threat (fear manipulation) along with coping mechanisms, and analyze the effects (from a fear-coping perspective) of manipulating both the threat and the coping mechanism on behavioral intention.

Second, this study extends the PMT model and incorporates privacy concern and personalisation into the conceptual model. The results showed both privacy concern and personalisation were significant in relation to protection motivation (i.e. intention to disclose personal information). Previous study on location-based services further suggests that other variables such as trust and risk are also important in influencing behavioral intention in information disclosure (Aloudat and Michael, 2011; Xu et al., 2011). It is recommended that future research incorporates other factors into the PMT model such as perceived risk, perceived benefits and trust, as well as test the model in different research contexts.

Finally, the revised PMT (Rogers, 1983) suggests both intrinsic and extrinsic rewards as important components of maladaptive rewards. Researchers (Rippetoe and Rogers, 1987, p599) describes an intrinsic maladaptive reward as when an individual has "appraised a dangerous situation as having no effective coping response, they either attempt to resign themselves to the situation or they put the predicament (difficulty) in the hands of God." In our study, the items for maladaptive rewards focused on extrinsic rewards. This was because in New Zealand, PMEAS is a relatively new service that has few current users; some PMEAS are also not available in all regions. In this situation, it would be difficult to systematically assess intrinsic rewards of not using PMEAS since most persons would not have experienced it either directly or indirectly (for example, through observation) so they can reasonably evaluate the intrinsic rewards this might bring. For example, intrinsic maladaptive reward could be assessed using indicators such as fatalism (i.e. the acceptance of a stressful situation as unchangeable and complacency in the face of danger because nothing can be done anyway.) and religious faith (i.e. use of one's spiritual beliefs and faith in God's will to cope with the possibility of threat occurrence). It is suggested that future study extends the current model to include intrinsic maladaptive rewards.

7.4 Concluding Comments

In summary, using Protection Motivation Theory (PMT) as the research framework, and supported by prior research on information disclosure (i.e. privacy and personalisation trade-off), this study sought to understand the factors that impact on individual's willingness to disclose personal information in the context of Personalised Mobile Emergency Alert Service (PMEAS).

Using survey data collected from mobile users in New Zealand, and analyzed using Partial Least Square (PLS) Path Modelling, empirical evidence was provided of the predictive power of PMT in the research context. In general, this study provides evidence that PMT together with the privacy-personalisation trade-off can be used to evaluate an individual's willingness to disclose personal information for the purpose of using PMEAS. The research findings further suggest that coping appraisal acts as the strongest predictor in the model, while threat appraisal was though impactful, inconsistent across different contexts. Personalisation and privacy concern were shown to be significant predictors of behavioral intention alongside the cognitive processes in PMT.

Taken altogether, the findings contribute valuable insights to the literature using PMT and to the emergency notification research. It also provides insights that can be used by PMEAS designers, service providers and government agencies as they design and implement better PMEAS for future use.

Bibliography

Acquisti, A., & Gross, R. (2006, June). Imagined communities: Awareness, information sharing, and privacy on the Facebook. *In International workshop on privacy enhancing technologies* (pp. 36-58). Springer Berlin Heidelberg.

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). *Privacy and human behavior in the age of information. Science, 347*(6221), 509-514.

Ada, S., Sharman, R., Han, W., & Brennan, J. A. (2016). Factors Impacting the Intention to Use Emergency Notification Services in Campus Emergencies: An Empirical Investigation. *IEEE Transactions on Professional Communication, 59*(2), 89-109.

Adomavicius, G., & Tuzhilin, A. (2005). Toward the next generation of recommender systems: A survey of the state-of-the-art and possible extensions. *IEEE transactions on knowledge and data engineering, 17*(6), 734-749.

Aloudat, A., & Michael, K. (2011). Toward the regulation of ubiquitous mobile government: a case study on location-based emergency services in Australia. *Electronic Commerce Research, 11*(1), 31-74.

Altman, I. (1975). *The environment and social behavior : privacy, personal space, territory, crowding*. Monterey, Calif.: Brooks/Cole Pub. Co.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *Mis Quarterly, 34*(3), 613-643.

Ardagna, C. A., Cremonini, M., di Vimercati, S. D. C., & Samarati, P. (2008). *Privacy-enhanced location-based access control. In Handbook of Database Security* (pp. 531-552). Springer US.

Arthur, D., & Quester, P. (2004). Who's afraid of that ad? Applying segmentation to the protection motivation model. *Psychology & Marketing, 21*(9), 671-696.

Atzmüller, C., & Steiner, P. M. (2010). Experimental vignette studies in survey research. *Methodology*.

Auckland Council. (2016). Aucklanders advised to change Civil Defence app. Retrieved Dec 20, 2016 from Our Auckland: http://ourauckland.aucklandcouncil.govt.nz/articles/news/2016/06/new-red-cross-hazard-app/

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS quarterly*, 13-28.

Báez, H., Vergara-Laurens, I., Torres-Molina, L., Jaimes, L. G., & Labrador, M. A. (2017, January). A real-time flood alert system for parking lots. *In Computing and Communication Workshop and Conference (CCWC), 2017 IEEE 7th Annual* (pp. 1-5). IEEE.

Bean, H., Liu, B. F., Madden, S., Sutton, J., Wood, M. M., & Mileti, D. S. (2016). Disaster Warnings in Your Pocket: How Audiences Interpret Mobile Alerts for an Unfamiliar Hazard. *Journal of Contingencies and Crisis Management, 24*(3), 136-147.

Beck, K. H. (1984). The effects of risk probability, outcome severity, efficacy of protection and access to protection on decision making: A further test of protection motivation theory. *Social Behavior and Personality: an international journal*, *12*(2), 121-125.

Bennett, P., Rowe, A., & Katz, D. (1998). Reported adherence with preventive asthma medication: a test of protection motivation theory. Psychology, health & medicine, 3(4), 347-354.

Beresford, A. R., & Stajano, F. (2003). Location privacy in pervasive computing. *IEEE Pervasive computing, 2(*1), 46-55.

Bockarjova, M., & Steg, L. (2014). Can Protection Motivation Theory predict pro-environmental behavior? Explaining the adoption of electric vehicles in the Netherlands. *Global environmental change, 28*, 276-288.

Boer H, Seydel E: Protection motivation theory, in Connor M, Norman P (eds.): *Predicting Health Behavior: Research and Practice With Social Cognition Models.* Buckingham, PA, Open University Press, 1996, pp. 95-120.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What Do Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors. *MIS Quarterly (MISQ), 39*(4), 837-864.

Bronfman, N. C., Cisternas, P. C., López-Vázquez, E., & Cifuentes, L. A. (2016). Trust and risk perception of natural hazards: implications for risk preparedness in Chile. *Natural Hazards, 81*(1), 307-327.

Cates, J. A., Dian, D. A., & Schnepf, G. W. (2003). Use of protection motivation theory to assess fear of crime in rural areas. *Psychology, Crime and Law, 9*(3), 225-236.

Chaikin, A. L., Derlega, V. J., & Miller, S. J. (1976). Effects of room environment on self-disclosure in a counseling analogue. *Journal of Counseling Psychology, 23*(5), 479.

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management, 6*(2-3), 181-202.

Chenoweth, T., Minch, R., & Gattiker, T. (2009, January). Application of protection motivation theory to adoption of protective technologies. In System Sciences, 2009. HICSS'09. *42nd Hawaii International Conference on* (pp. 1-10). IEEE.

Choy, S., Handmer, J., Whittaker, J., Shinohara, Y., Hatori, T., & Kohtake, N. (2016). Application of satellite navigation system for emergency warning and alerting. *Computers, Environment and Urban Systems, 58*, 12-18.

Conner, M., & Norman, P. (2005). *Predicting health behaviour: Research and practice with social cognition models* (2nd ed.). New York;Maidenhead, England;: Open University Press.

Christofides, E., Muise, A., & Desmarais, S. (2009). Information disclosure and control on Facebook: are they two sides of the same coin or two different processes?. *CyberPsychology & Behavior, 12*(3), 341-345.

Chua, W. F. (1986). Radical Developments in Accounting Thought. *The Accounting Review, 61*(4), 601-632.

Cismaru, M., & Lavack, A. M. (2006). Marketing communications and protection motivation theory: Examining consumer decision-making. *International Review on Public and Nonprofit Marketing, 3*(2), 9-24.

Cismaru, M., & Lavack, A. M. (2007). Interaction effects and combinatorial rules governing protection motivation theory variables: A new model. *Marketing Theory, 7*(3), 249-270.

Crossler, R. E., Long, J. H., Loraas, T. M., & Trinkle, B. S. (2014). Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap. *Journal of Information Systems, 28*(1), 209-226.

CRS Report for Congress. (2011, 4 6). Japan's 2011 Earthquake and Tsunami: Economic Effects and Implications for the United States. Retrieved Dec 1, 2016, from FAS.ORG: https://fas.org/sgp/crs/row/R41702.pdf

Dinev, T., & Hart, P. (2003, August). PRIVACY CONCERNS AND INTERNET USE--A MODEL OF TRADE-OFF FACTORS. *In Academy of Management Proceedings* (Vol. 2003, No. 1, pp. D1-D6). Academy of Management.

Dinev, T., & Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce, 10*(2), 7-29.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61-80.

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance–An empirical investigation. *The Journal of Strategic Information Systems*, *17*(3), 214-233.

Dwyer, C., Hiltz, S., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. *AMCIS 2007 proceedings*, 339.

Early Warning Network (2017). Retrieved Apr 6, 2017 from http://www.ewn.com.au/

Federal Communications Commission. (2016). Wireless Emergency Alerts (WEA). Retrieved Nov 10, 2016 from https://www.fcc.gov/consumers/guides/wireless-emergency-alerts-wea

Federal Information & News Dispatch, I. (2015). Review of the emergency alert system. Retrieved Nov 10, 2016 from: https://www.fcc.gov/document/review-emergency-alert-system-1

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of applied social psychology, 30*(2), 407-429.

Fritz, C. E., & Marks, E. S. (1954). The NORC studies of human behavior in disaster. *Journal of Social Issues*, 10(3), 26-41.

Fry, R. B., & Prentice-Dunn, S. (2006). Effects of a psychosocial intervention on breast self-examination attitudes and behaviors. *Health education research, 21*(2), 287-295.

GAR. (2015). *Global Assessment Report on Disaster Risk Reduction*. Geneva, Switzerland: United Nations Office for Disaster Risk Reduction (UNISDR).

GFDRR. (2016). *The making of a riskier future: How our decisions are shaping future disaster risk.* Washington, D.C.: Global Facility for Disaster Reduction and Recovery

Gutierrez, D. (2008) Natural Disasters Up More Than 400 Percent in Two Decades. Retrieved Apr 4, 2017, from Natural News: http://www.naturalnews.com/023362.html

Haataja, M., Häkkinen, M., & Sullivan, H. (2011, May). Understanding user acceptance of mobile alerting systems. In *Proceedings of the 8th International ISCRAM Conference*.

Hair, J. F., Hult G. M., Ringle, C. M., Sarstedt, M. (2014). *A primer on partial least squares structural equation modeling (PLS-SEM).* Thousand Oaks, Calif: SAGE Publications.

Hair, J. F., Hult G. M., Ringle, C. M. (2017). *A primer on partial least squares structural equation modeling (PLS-SEM).* Thousand Oaks, Calif: SAGE Publications.

Haiti Earthquake: Facts, D. E. (2015, 10 26). Haiti Earthquake: Facts, Damage, Effects on Economy. Retrieved Dec 4, 2016, from the balance: https://www.thebalance.com/haiti-earthquake-facts-damage-effects-on-economy-3305660

Han, W., Ada, S., Sharman, R., Gray, R. H., & Simha, A. (2014). Factors impacting the adoption of social network sites for emergency notification purposes in

universities. International *Journal of Business Information Systems*, *18*(1), 85-106.

Han, W., Ada, S., Sharman, R., & Rao, H. R. (2015). Campus Emergency Notification Systems: An Examination of Factors Affecting Compliance with Alerts. *Mis Quarterly*, *39*(4), 909-929.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106-125.

Hilton, S., Anderson, H. R., Sibbald, B., & Freeling, P. (1986). Controlled evaluation of the effects of patient education on asthma morbidity in general practice. *The Lancet*, *327*(8471), 26-29.

Hovland, C. I., Janis, I. L., & Kelley, H. H. (1953). Communication and persuasion; *psychological studies of opinion change*.

Hunter, C. E., Ballou, B. L., Hebrank, J. H., Fallon, J., Summer, R. D., & McNeil, L. (2007). *U.S. Patent No. 7,233,781*. Washington, DC: U.S. Patent and Trademark Office.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83-95.

James, T. L., Warkentin, M., & Collignon, S. E. (2015). A dual privacy decision model for online social networks. *Information & Management*, *52*(8), 893-908.

Janis, I. L. (1967). Effects of fear arousal on attitude change: Recent developments in theory and experimental research. *Advances in experimental social psychology*, *3*, 166-224.

Japan Meteorological Agency (2007). Earthquake Early Warning System. Retrieved Nov 18, 2016 from http://www.jma.go.jp/jma/en/Activities/eew.html

Jarvenpaa, S. L., Tractinsky, N., & Saarinen, L. (1999). Consumer trust in an internet store: a cross-cultural validation. *Journal of Computer-Mediated Communication*, *5*(2), 0-0.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS quarterly*, 549-566.

Junglas, I. A., Johnson, N. A., & Spitzmüller, C. (2008). Personality traits and concern for privacy: an empirical study in the context of location-based services. *European Journal of Information Systems, 17*(4), 387-402.

Junglas, I., & Watson, R. T. (2006). The u-constructs: four information drives. *Communications of the Association for Information systems, 17*(1), 26.

Junn, J. (2017, 3 23). Using virtual reality to help save lives in a real fire. Retrieved Apr 10, 2017 from Idealog: http://idealog.co.nz/design/2017/03/using-virtual-reality-help-save-lives-real-fire

Keselman, H. J., Huberty, C. J., Lix, L. M., Olejnik, S., Cribbie, R. A., Donahue, B., ... & Levin, J. R. (1998). Statistical practices of educational researchers: An analyss of their ANOVA, MANOVA, and ANCOVA analyses. *Review of Educational Research, 68*(3), 350-386.

Kim, D., & Mousavizadeh, M. (2015). A Study of the Effect of Privacy Assurance Mechanisms on Self-disclosure in Social Networking Sites from the View of Protection Motivation Theory. *Emergent Research Forum Papers*.

Kim, E., & Lee, B. (2009). E-service quality competition through personalization under consumer privacy concerns. *Electronic Commerce Research and Applications, 8*(4), 182-190.

Kim, S., Jeong, S. H., & Hwang, Y. (2013). Predictors of pro-environmental behaviors of American and Korean students: The application of the theory of reasoned action and protection motivation theory. Science Communication, 35(2), 168-188.

Kobsa, A. (2007). Privacy-enhanced personalization. Communications of the *ACM, 50*(8), 24-33.

Krug, K., Mountain, D., & Phan, D. (2003). Location-based services for mobile users in protected areas. *GeoInformatics, 6*(2), 26-29

Lee, C. H., & Cranage, D. A. (2011). Personalisation–privacy paradox: The effects of personalisation and privacy assurance on customer responses to travel web sites. *Tourism Management, 32*(5), 987-994.

Lee, Y. (2011). Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective. *Decision Support Systems, 50*(2), 361-369.

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. European Journal of Information Systems, 18(2), 177-187.

Leventhal, H. (1970). Findings and theory in the study of fear communications. *Advances in experimental social psychology, 5*, 119-186.

Li, H., Sarathy, R., & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems, 51*(3), 434-445.

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems, 54*(1), 471-481.

LII. (2016). U.S. Code. Title 42, Chapter 68, Subchapter I, §5122. Retrieved Dec 20, 2016 from https://www.law.cornell.edu/uscode/text

Liu, C. F. (2011). Key factors influencing the intention of telecare adoption: An institutional perspective. *Telemedicine and e-Health, 17*(4), 288-293.

Lo, J. (2010). Privacy Concern, Locus of Control, and Salience in a Trust-Risk Model of Information Disclosure on Social Networking Sites. *In AMCIS* (p. 110).

Lowry, P. B., Cao, J., & Everard, A. (2011). Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of Management Information Systems, 27(*4), 163-200.

Lucy Pearson. (2012, 11 21). Early Warning of Disaster: Facts and Figures. Retrieved Oct 12, 2016 from Sci Dev Net: http://www.scidev.net/global/communication/feature/early-warning-of-disasters-facts-and-figures-1.html

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of experimental social psychology, 19*(5), 469-479.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research, 15*(4), 336-355.

McClendon, B. T., & Prentice-Dunn, S. (2001). Reducing skin cancer risk: an intervention based on protection motivation theory. *Journal of health psychology, 6*(3), 321-328.

McGee, T. K., & Gow, G. A. (2012). Potential responses by on-campus university students to a university emergency alert. *Journal of Risk Research, 15*(6), 693.

McGrath, J. E. (1981). Dilemmatics: The study of research choices and dilemmas. *American Behavioral Scientist, 25*(2), 179-210.

McGuire, W. J. (1969). The nature of attitudes and attitude change. *The handbook of social psychology, 3(*2), 136-314.

Melamed, S., Rabinowitz, S., Feiner, M., Weisberg, E., & Ribak, J. (1996). Usefulness of the protection motivation theory in explaining hearing protection device use among male industrial workers. *Health psychology, 15*(3), 209.

Menard, P., Gatlin, R., & Warkentin, M. (2014). Threat protection and convenience: Antecedents of cloud-based data backup. *Journal of Computer Information Systems, 55*(1), 83-91.

Meso, P., Ding, Y., & Xu, S. (2013). Applying protection motivation theory to information security training for college students. *Journal of Information Privacy and Security, 9*(1), 47-67.

Milne, G. R., & Gordon, M. E. (1993). Direct mail privacy-efficiency trade-offs within an implied social contract framework. *Journal of Public Policy & Marketing, 12*(2), 206-215.

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology, 30*(1), 106-143.

Milne, S., Orbell, S., & Sheeran, P. (2002). Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions. *British journal of health psychology, 7*(2), 163-184.

Mulilis, J. P., & Lippa, R. (1990). Behavioral change in earthquake preparedness due to negative threat appeals: A test of protection motivation theory. *Journal of Applied Social Psychology, 20*(8), 619-638.

Murgraff, V., White, D., & Phillips, K. (1999). An application of protection motivation theory to riskier single-occasion drinking. *Psychology and Health, 14*(2), 339-350.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*, *18*(2), 126-139.

National Business Research Institution. (2016). METHODS OF SURVEY DATA COLLECTION. Retrieved Nov 10, 2016 from https://www.nbrii.com/customer-survey-white-papers/methods-of-survey-data-collection/

NASA. (2013). NASA HQ Emergency Management Program. Retrieved Apr 10, 201 from NASA: https://www.nasa.gov/centers/hq/emergency/hqEmergencyMgmtPrgm/#.WOpEEWmGPIU

National Oceanic and Atmospheric Administration (2014). Wireless Emergency Alerts: Real Stories. Retrieved Feb 6, 2017 from National Weather Service: http://www.nws.noaa.gov/com/weatherreadynation/news/130313_wea_stories.html

Davies, R. (2017). New Zealand – Over 300 Homes Damaged as More Flooding Hits North Island. Retrieved Mar 30, 2017 from Floodlist: http://floodlist.com/australia/new-zealand-north-island-floods-march-2017

Norberg, P. A., Horne, D. A., & Horne, D. R. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *The Journal of Consumer Affairs*, *41*(1), 100-126.

Norman, P., Searle, A., Harrad, R., & Vedhara, K. (2003). Predicting adherence to eye patching in children with amblyopia: an application of protection motivation theory. *British journal of health psychology, 8*(1), 67-82.

Nazarov, E. (2011). Emergency response management in japan. *Azerbaijan: Crisis Management Center, Ministry of Emergency Situations of the Republic of Azerbaijan*.

OECD. (2012). Development: Aid to developing countries falls because of global recession. Retrieved Sep 12, 2016 from http://www.oecd.org/newsroom/developmentaidtodevelopingcountriesfallsbecauseofglobalrecession.htm

Palen, L., Anderson, K. M., Mark, G., Martin, J., Sicker, D., Palmer, M., & Grunwald, D. (2010, April). A vision for technology-mediated support for public participation & assistance in mass emergencies & disasters. *In Proceedings of the 2010 ACM-BCS visions of computer science conference* (p. 8). British Computer Society.

Pavlou, P. A. (2011). State of the information privacy literature: where are we now and where should we go? *MIS quarterly*, *35*(4), 977-988.

Pechmann, C., Zhao, G., Goldberg, M. E., & Reibling, E. T. (2003). What to convey in antismoking advertisements for adolescents: The use of protection motivation theory to identify effective message themes. *Journal of Marketing, 67*(2), 1-18.

Perloff, R. M. (2010). *The dynamics of persuasion: communication and attitudes in the twenty-first century*. Routledge.

Petronio, S. (2012). *Boundaries of privacy: Dialectics of disclosure*. Suny Press.

Plotnikoff, R. C., & Higginbotham, N. (1998). Protection motivation theory and the prediction of exercise and low-fat diet behaviours among Australian cardiac patients. *Psychology and Health*, *13*(3), 411-429.

Plotnikoff, R. C., & Higginbotham, N. (2002). Protection motivation theory and exercise behaviour change for the prevention of heart disease in a high-risk, Australian representative community sample of adults. *Psychology, health & medicine, 7*(1), 87-98.

Plotnikoff, R. C., Trinh, L., Courneya, K. S., Karunamuni, N., & Sigal, R. J. (2009). Predictors of aerobic physical activity and resistance training among Canadian adults with type 2 diabetes: An application of the Protection Motivation Theory. *Psychology of Sport and Exercise*, *10*(3), 320-328.

Prentice-Dunn, S., & Rogers, R. W. (1986). Protection motivation theory and preventive health: Beyond the health belief model. *Health education research, 1*(3), 153-161.

Prentice-Dunn, S., Mcmath, B. F., & Cramer, R. J. (2009). Protection motivation theory and stages of change in sun protective behavior. *Journal of Health Psychology, 14*(2), 297-305.

Rahaei, Z., Ghofranipour, F., Morowatisharifabad, M. A., & Mohammadi, E. (2015). Determinants of cancer early detection behaviors: application of protection motivation theory. *Health promotion perspectives, 5*(2), 138.

Rao, A., Schaub, F., Sadeh, N., Acquisti, A., & Kang, R. (2016, January). Expecting the unexpected: Understanding mismatched privacy expectations online. In *Symposium on Usable Privacy and Security (SOUPS)*.

Rapid Notify (2017). Emergency and Mass Notification. Retrieved Apr 8, 2017 from http://www.rapidnotify.com/services.html

Ren, Y., Kiesler, S., & Fussell, S. R. (2008). Multiple group coordination in complex and dynamic task environments: Interruptions, coping mechanisms, and technology recommendations. *Journal of Management Information Systems, 25*(1), 105-130.

Rippetoe, P. A., & Rogers, R. W. (1987). Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat. Journal of personality and social psychology, 52(3), 596.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. The journal of psychology, 91(1), 93-114.

Rogers, R. W., & Prentice-Dunn, S. (1997). Protection motivation theory. In D. Gochman (Ed.), *Handbook of health behavior research*: Vol. 1. *Determinants of health behavior: Personal and social* (pp. 113-132). New York, NY Plenum.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social psychophysiology*, 153-176.

Ruthig, J. C. (2016). Health risk perceptions and exercise in older adulthood: An application of protection motivation theory. *Journal of Applied Gerontology, 35*(9), 939-959.

Salleh, N., Hussein, R., Mohamed, N., Karim, N. S. A., Ahlan, A. R., & Aditiawarman, U. (2012). Examining information disclosure behavior on social network sites

using protection motivation theory, trust and risk. *Journal of Internet Social Networking & Virtual Communities, 2012*, 1.

Salleh, N., Hussein, R., Mohamed, N., & Aditiawarman, U. (2013, December). An empirical study of the factors influencing information disclosure behaviour in social networking sites. *In Advanced Computer Science Applications and Technologies (ACSAT), 2013 International Conference on* (pp. 181-185). IEEE.

Sanquist, T. F., Mahy, H., & Morris, F. (2008). An exploratory risk perception study of attitudes toward homeland security systems. *Risk analysis*, *28*(4), 1125-1133.

Seaborn, J. G. C. (1975). *U.S. Patent No. 3,914,692*. Washington, DC: U.S. Patent and Trademark Office.

Sheehan, K. B. (2002). Toward a typology of Internet users and online privacy concerns. *The Information Society*, *18*(1), 21-32.

Siponen, M., Pahnila, S., & Mahmood, A. (2006, November). Factors influencing protection motivation and IS security policy compliance. *In Innovations in Information Technology, 2006* (pp. 1-5). IEEE.

Smith, H. J., Dinev, T., & Xu, H. (2011). INFORMATION PRIVACY RESEARCH: AN INTERDISCIPLINARY REVIEW. *MIS Quarterly, 35*(4), 989.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly, 20*(2), 167-196.

Stanley, M. A., & Maddux, J. E. (1986). Cognitive processes in health enhancement: Investigation of a combined protection motivation and self-efficacy model. *Basic and Applied Social Psychology*, *7*(2), 101-113.

Stone, E. F., & Stone, D. L. (1990). Privacy in organizations: Theoretical issues, research findings, and protection mechanisms. *Research in personnel and human resources management*, *8*(3), 349-411.

Stuff. (2010, 01 14). Haiti earthquake damage 'staggering'. Retrieved Sep 5, 2016 from Stuff: http://www.stuff.co.nz/world/americas/3226761/Haiti-earthquake-damage-staggering

Stuff. (2017). Edgecumbe township evacuated as flood bank breached. Retrieved Apr 8, 2017 from http://www.stuff.co.nz/national/91174483/live-heavy-rain-brings-flooding-as-cyclone-debbie-remnants-hit-nz

Stuff. (2017). Emergency phone alerts system fast-tracked despite technology concerns. Retrieved Apr 6, 2017 from http://www.stuff.co.nz/national/politics/90194009/emergency-phone-alerts-system-fasttracked-despite-technology-concerns

Su, S. P., Tsai, C. H., & Hsu, W. L. (2013). Extending the TAM Model to Explore the Factors Affecting Intention to Use Telecare Systems. *JCP, 8*(2), 525-532.

Sun, Y., La Porta, T. F., & Kermani, P. (2009). A flexible privacy-enhanced location-based services system framework and practice. *IEEE Transactions on Mobile Computing, 8*(3), 304-321.

Tannenbaum, M. B., Hepler, J., Zimmerman, R. S., Saul, L., Jacobs, S., Wilson, K., & Albarracín, D. (2015). Appealing to fear: A meta-analysis of fear appeal effectiveness and theories. *Psychological Bulletin, 141*(6), 1178-1204.

Taylor, A. H., & May, S. (1996). Threat and coping appraisal as determinants of compliance with sports injury rehabilitation: an application of protection motivation theory. *Journal of sports sciences, 14*(6), 471-482.

The Southland Times. (2015). Cellphones instead of sirens will alert Southlanders of emergencies. Retrieved Jan 25, 2017 from http://www.stuff.co.nz/southland-times/news/68834772/Cellphones-instead-of-sirens-will-alert-Southlanders-of-emergencies

Tsai, H. Y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security, 59*, 138-150.

Tupler, A. M., & Mock, V. A. (2007). *U.S. Patent No. 7,212,111*. Washington, DC: U.S. Patent and Trademark Office.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management, 49*(3), 190-198.

Vinzi, V. E., Chin, W. W., Henseler, J., & Wang, H. (Eds.). (2010). *Handbook of partial least squares: Concepts, methods and applications*. Springer Science & Business Media.

Weber, R. (2004). The rhetoric of positivism versus interpretivism: a personal view. *MIS Quarterly, 28*(1), iii.

Weng, Y. (2003). *U.S. Patent Application No. 10/639,806*.

Whalen, D. J. (1996). *I see what you mean: Persuasive business communication*. Sage.

Wildavsky, A., & Dake, K. (1990). Theories of risk perception: Who fears what and why?. *Daedalus*, 41-60.

Wilde, C. (2013, 6 28). Complacency, apathy lead people to ignore disaster warnings, researchers say. Retrieved Nov 20, 2016 from University of Buffalo: http://www.buffalo.edu/news/releases/2013/06/048.html

Witte, K., & Allen, M. (2000). A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health Education & Behavior, 27*(5), 591-615.

Wolf, S., Gregory, W. L., & Stephan, W. G. (1986). Protection Motivation Theory: Prediction of Intentions to Engage in Anti-Nuclear War Behaviors1. *Journal of Applied Social Psychology, 16*(4), 310-321.

Wong, K. K. (2015). Mediation analysis, categorical moderation analysis, and higher-order constructs modeling in Partial Least Squares Structural Equation Modeling (PLS-SEM): A B2B Example using SmartPLS. *Unpublished manuscript. Retrieved on, 25*.

Woon, I., Tan, G. W., & Low, R. (2005). A protection motivation theory approach to home wireless security. *ICIS 2005 proceedings*, 31.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in human behavior, 24*(6), 2799-2816.

WHO. (2016). Definitions: emergencies. Retrieved Nov 20, 2016 from World Health Organization: http://www.who.int/hac/about/definitions/en/

Wu, P. Qu, Y. & Preece, J. (2008). Why an Emergency Alert System isn't Adopted: The Impact of SocioTechnical Context. *In Proceedings of the 22nd Human Computer Interaction Conference*. Liverpool, UK.

Wurtele, S. K. (1988). Increasing Women's Calcium Intake: The Role of Health Beliefs, Intentions, and Health Value1. *Journal of Applied Social Psychology, 18*(8), 627-639.

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. *ICIS 2008 proceedings*, 6.

Xu, H., Luo, X., Carroll, J. M., & Rosson, M. B. (2011). The personalisation privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems, 51*(1), 42-52.

Xu, H., Teo, H. H., Tan, B. C., & Agarwal, R. (2009). The role of push-pull technology in privacy calculus: the case of location-based services. *Journal of Management Information Systems, 26*(3), 135-174.

Xu, H., Teo, H. H., Tan, B. C., & Agarwal, R. (2012). Research note—effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services. *Information Systems Research*, *23*(4), 1342-1363.

Yan, Y., Jacques-Tiura, A. J., Chen, X., Xie, N., Chen, J., Yang, N., ... & MacDonell, K. K. (2014). Application of the Protection Motivation Theory in predicting cigarette smoking among adolescents in China. *Addictive behaviors*, *39*(1), 181-188.

Yang, C. G., & Lee, H. J. (2016). A study on the antecedents of healthcare information protection intention. *Information Systems Frontiers, 18*(2), 253-263.

Yang, Z., Peterson, R. T., & Cai, S. (2003). Services quality dimensions of Internet retailing: an exploratory analysis. *Journal of Services Marketing, 17*(7), 685–700.

Young, A. L., & Quan-Haase, A. (2009, June). Information revelation and internet privacy concerns on social network sites: a case study of facebook. In *Proceedings of the fourth international conference on Communities and technologies* (pp. 265-274). ACM.

Zeithaml, V. A., Berry, L. L., & Parasuraman, A. (1996). The behavioral consequences of service quality. *the Journal of Marketing*, 31-46.

Zeithaml, V. A., Parasuraman, A., & Malhotra, A. (2000). Conceptual Framework for understanding e-service quality: Implications for future research and managerial practice

Zeithaml, V. A., Rust, R. T., & Lemon, K. N. (2001). The customer pyramid: creating and serving profitable customers. *California Management Review*, *43*(4), 118-142.

Zhao, L., Lu, Y., & Gupta, S. (2012). Disclosure intention of location-related information in location-based social network services. *International Journal of Electronic Commerce*, *16*(4), 53-90.

Appendix A. Survey Information Sheet

Contact Details

Researcher: Jing Zhang
(jing.zhang@pg.canterbury.ac.nz)

Supervisor: Assoc. Prof. Annette Mills
(annette.mills@canterbury.ac.nz)

UNIVERSITY OF CANTERBURY
Te Whare Wānanga o Waitaha
CHRISTCHURCH NEW ZEALAND

You are invited to participate in a research project on **Personalised Mobile Emergency Alert Service (MEAS)**. Personalised MEAS is a public service system that uses GPS technology and other personal information to provide personalised emergency alerts (e.g. earthquake, flood, etc.) to individual mobile devices. The aim of this research is to understand what would encourage people to disclose personal and location-based information in order to receive personalised emergency alerts on their mobile devices.

This project is being carried out as a requirement for a Masters of Commerce by Jing Zhang (jing.zhang@pg.canterbury.ac.nz) under the supervision of Associate Professor Annette Mills, who can be contacted at annette.mills@canterbury.ac.nz. She will be pleased to discuss any concerns you may have about participation in the project.

This survey is anonymous, and you will not be identified. Participation in this study is voluntary, and you may stop and withdraw any information you have provided, up until the survey has been submitted and added to the other data collected. As the survey is anonymous, your data cannot be withdrawn once it has been combined with the other data collected.

By completing this survey it will be understood that you have consented to participate in this project, and that you consent to publication of the results of the project with the understanding that your anonymity will be preserved.

A thesis is a public document and will be available through the UC Library. You may

also request a copy of the results at the conclusion of this research. To receive a copy of the results, please email the researcher, Jing Zhang at jing.zhang@pg.canterbury.ac.nz.

This project has been reviewed and approved by the University of Canterbury Human Ethics Committee, and participants should address any complaints to:

The Chair,
Human Ethics Committee,
University of Canterbury, Private Bag 4800, Christchurch
email: humanethics@canterbury.ac.nz

Participants could refer to the following support service should they feel distressed or uncomfortable during survey:

Petersgate Counselling Center
Phone: 03-343-3391
29 Yaldhurst Road, Upper Riccarton,
Christchurch, 8042

Thank you for your participation in this research project.

Appendix B. Survey Questions

Introduction

This survey is aimed at individuals who have access to a **mobile device** (e.g. mobile phone, tablet) that can potentially receive **personalised emergency alerts**. This survey should take approximately 10-15 minutes to complete.

For each question, please select the response that you feel is appropriate and is to the best of your knowledge. If you find it difficult to determine your exact answer, please give your best estimate. Your participation in this study is entirely voluntary and you can withdraw at any time. You are free to omit any question.

Some questions may appear very similar. This is intentional to ensure greater statistical reliability and accuracy. We would therefore greatly appreciate if you would answer all questions.

Key Terms

Personalised Mobile Emergency Alert Service (MEAS) is public safety service systems that provide emergency alerts before or during an emergency to mobile devices. This service is used by **governments** and **authorized communication technology companies** around the world. It enables people to take actions when they receive alerts.

Mobile Emergency Alerts are text-like messages that are sent to users' mobile devices in case of emergency. The types of emergency alerts include but not limited to severe weather information, natural hazards, imminent threats, national security and local incident information. The alerts typically show the emergency type and duration, any action you should take and the emergency service provider issuing the alert. For example: "Flood warning for lower Christchurch till 1:00PM. Prepare. Avoid Travel. Check media. Canterbury CD."

To receive the alerts, individuals would sign up to the service through a mobile device which enables the service provider to tailor the alert messages and recommended actions to the user based on their location (both registered location and current location) and other relevant personal information such as gender, age and health information if disclosed.

Q1: Approximately how long have you been using a mobile device? _____ Year(s)

Q2: To what extent do you use Wi-Fi on your mobile device?

- ❍ Never
- ❍ Rarely
- ❍ Occasionally
- ❍ Sometimes
- ❍ Frequently
- ❍ Very Frequently
- ❍ Always

Q3: To what extent do you use mobile data?

- ❍ Never
- ❍ Rarely
- ❍ Occasionally
- ❍ Sometimes
- ❍ Frequently
- ❍ Very Frequently
- ❍ Always

Q4: Do you use an emergency alert service on your mobile device?

- ❍ Yes. (Please answer Q4.1 and Q4.2)
- ❍ No. (Please skip to Q4.3)

Q4.1 Please name the emergency alert service you most often use on your mobile device.

_____

Q4.2: How often do you use an emergency alert service on your mobile device?

- ❍ Never
- ❍ Rarely
- ❍ Occasionally
- ❍ Sometimes
- ❍ Frequently
- ❍ Very Frequently
- ❍ Always

Q4.3: Is the mobile emergency alert service that you use based on your location?

- ❍ Yes
- ❍ No

Q5: Location-Based Services (LBS) are applications that use your location (e.g. GPS data) to provide information or services that are relevant to that location (e.g. restaurants recommended in the location where you are). To what extent do you use Location-Based services?

- ❍ Never
- ❍ Rarely
- ❍ Occasionally
- ❍ Sometimes
- ❍ Frequently
- ❍ Very Frequently
- ❍ Always

Potential Emergencies

The following set of questions relate to potential emergencies.

Emergency Scenario #1: Storm

The National Weather Service issues a storm watch for portions of your country, which includes your region. Heavy rains have been falling for three hours. The storm system is moving towards where you

live. High winds and flooding have been reported in some areas. Consider the emergency situation described above:

Q1: To what extent do you agree or disagree with the statements below?

(-3= “Strongly Disagree”, 0= “Neither”, +3= “Strong Agree”)

If I were affected by an emergency situation like this:

1) ... it would be severe.

2) ... it would be serious.

3) ...it would be problematic.

4) If I were affected by an emergency situation like this, I would suffer a lot.

5) Being affected by an emergency situation like this would be likely to cause me major problems.

Q2: To what extent do you agree or disagree with the statements below?

(-3= “Strongly Disagree”, 0= “Neither”, +3= “Strong Agree”)

1) My chances of being affected by an emergency situation like this in the future are high.

2) It is possible that I will be affected by an emergency situation like this.

3) I am at risk of being affected by an emergency situation like this in the future.

4) It is likely that I will be affected by an emergency situation like this.

5) My chances of being affected by an emergency situation like this in the future are high.

Q3: To what extent do you agree or disagree with the statements below?

The prospect of being affected by an emergency situation like this would make me:

(-3= “Strongly Disagree”, 0= “Neither”, +3= “Strong Agree”)

1) ... worried.

2) ... anxious.

3) ... scared.

4)... frightened.

Emergency Scenario #2: Earthquake

A magnitude 6.0 earthquake happened about 20km from your location (at a depth of 10km). Strong ground shaking from the main shock lasted for approximately 45 seconds in some areas. Aftershocks of

varying intensity will be felt throughout the region for several days following the main shock, causing further damage to structures that were already damaged or weakened by the previous shaking.

Q1: To what extent do you agree or disagree with the statements below?

(-3= “Strongly Disagree”, 0= “Neither”, +3= “Strong Agree”)

If I were affected by an emergency situation like this:

1) ... it would be severe.

2) ... it would be serious.

3) ...it would be problematic.

4) If I were affected by an emergency situation like this, I would suffer a lot.

5) Being affected by an emergency situation like this would be likely to cause me major problems.

Q2: To what extent do you agree or disagree with the statements below?

(-3= “Strongly Disagree”, 0= “Neither”, +3= “Strong Agree”)

1) My chances of being affected by an emergency situation like this in the future are high.

2) It is possible that I will be affected by an emergency situation like this.

3) I am at risk of being affected by an emergency situation like this in the future.

4) It is likely that I will be affected by an emergency situation like this.

5) My chances of being affected by an emergency situation like this in the future are high.

Q3: To what extent do you agree or disagree with the statements below?

The prospect of being affected by an emergency situation like this would make me:

(-3= “Strongly Disagree”, 0= “Neither”, +3= “Strong Agree”)

1) ... worried.

2) ... anxious.

3) ... scared.

4)... frightened.

Potential use of Personalised MEASA personalised

MEAS can provide personalised emergency alerts based on your location and other personal information that you may provide to the system to increase personalisation.

The following set of questions relate to your intention to use a personalised Mobile Emergency Alert Service (MEAS) if it is available to you.

Q1: Which of the following information would you be willing to disclose in order to use a personalised MEAS?

1. Personal Details (Tick all that apply)

- ❑ Name
- ❑ Age
- ❑ Gender
- ❑ Disabilities
- ❑ Health information
- ❑ Body statistics (e.g. height, weight)
- ❑ Household composition and relationships (e.g. one-person household, one or multi-family household, a group of people)
- ❑ None of the above
- ❑ Other (Please Specify) _____

2. Contact Details (Tick all that apply)

- ❑ E-mail address
- ❑ (Mobile) Phone number
- ❑ (Home) Phone number
- ❑ (Work) Phone number
- ❑ Emergency contact (e.g. next of kin)
- ❑ None of the above
- ❑ Other (Please Specify) _____

3. Location Information (Tick all that apply)

- ❑ GPS location of your mobile device
- ❑ Your registered location of interest
- ❑ Your registered location of family or friends (to receive other alerts)
- ❑ Your home address
- ❑ Your postal code or suburb
- ❑ Town or city
- ❑ None of the above
- ❑ Other (Please Specify) _____

Q2: To what extent do you agree or disagree with the statements below?

(-3= "Strongly Disagree", 0= "Neither", +3= "Strong Agree")

If personalised Mobile Emergency Alert Service (MEAS) were available to you:

1) ... I intend to use a personalised MEAS.

2) ... I plan to use a personalised MEAS.

3)... I predict I would use a personalised MEAS.

Self-Efficacy & Response Efficacy

The following set of questions relate to your beliefs about using a personalised Mobile Emergency Alert Service (MEAS).

Q1: To what extent do you agree or disagree with the statements below?

(-3= "Strongly Disagree", 0= "Neither", +3= "Strong Agree")

1) Using a personalised MEAS would be a good way to reduce my risk of being affected by an emergency situation.

2) I feel confident in my ability to use a personalised MEAS.

3) Using a personalised MEAS would lessen my chances of being affected by an emergency situation.

4) I have the resources necessary to use a personalised MEAS.

5) Using a personalised MEAS would be effective for protecting me from being affected by an emergency situation.

6) I have the knowledge necessary to use a personalised MEAS.

Cost of Using Personalised MEAS

The following set of questions relate to your beliefs about the effort, time and cost needed to use a personalised Mobile Emergency Alert Service (MEAS).

Q1: To what extent do you agree or disagree with the statements below?

(-3= "Strongly Disagree", 0= "Neither", +3= "Strong Agree")

1) Mobile data for using a location-based service like personalised MEAS would be costly.

2) It would be time-consuming to set up a personalised MEAS (e.g. providing my personal data such as name, address, health status, etc.).

3) It would be time-consuming to maintain my personal profile in a personalised MEAS (e.g. updating my mobile number, address, health status, etc.).

4) Using a personalised MEAS may cause problems with other applications on my mobile device(s).

5) Using a personalised MEAS would require considerable investment of effort other than time.

6) There are too many costs associated with using a location-based service like personalised MEAS.

Q2: To what extent do you agree or disagree with the statements below?

(-3= "Strongly Disagree", 0= "Neither", +3= "Strong Agree")

Not using a personalised MEAS would:

1) ... save me time.

2) ... save me money.

3) ... save me effort.

4) ... avoid false alarms.

5) ... save me from taking unnecessary actions.

6) ... avoid unnecessary disruption.

Personalisation

The following set of questions relate to your beliefs about personalisation of a Mobile Emergency Alert Service (MEAS).

Q1: To what extent do you agree or disagree with the statements below?

(-3= "Strongly Disagree", 0= "Neither", +3= "Strong Agree")

A personalised MEAS could provide me with:

1) ... emergency alert information that is tailored to my personal needs.

2) ... the kind of emergency alert information that I might need.

3) ... emergency alert information that is specific to my situation.

Information Privacy

The following set of questions relate to your beliefs about information privacy in relation to providing information to a personalised Mobile Alert Service (MEAS) provider.

Q1: To what extent do you agree or disagree with the statements below?

(-3= "Strongly Disagree", 0= "Neither", +3= "Strong Agree")

1) It would bother me if a personalised MEAS provider were to ask me for personal information.

2) If a personalised MEAS provider asks me for personal information, I would think twice before providing it.

3) I would be concerned that a MEAS provider would be collecting too much information about me.

Personal Innovativeness

To what extent do you agree or disagree with the statements below?

(-3= "Strongly Disagree", 0= "Neither", +3= "Strong Agree")

1) If I heard about a new information technology, I would look for ways to experiment with it.

2) Among my peers, I am usually the first to try out new information technologies.

3) I like to experiment with new information technologies.

Prior Experience

(-3= “Not at All”, 0= “Neither”, +3= “Very Often”)

1) How often have you personally been a victim of what you felt was an invasion of privacy?

2) How often have you received a false alarm for an emergency?

Demographics

Please provide information about yourself in the following set of questions. This information will be used for statistical purposes only, and you will not be identified.

Q1: Age

- ❍ Under 20 years
- ❍ 20-24 years
- ❍ 25-29 years
- ❍ 30-34 years
- ❍ 35-39 years
- ❍ 40-49 years
- ❍ 50-59 years
- ❍ 60 years and above

Q2: Gender

- ❍ Male
- ❍ Female
- ❍ Other
- ❍ Prefer not to say

Q3: Which of the following best describes your highest level of education?

- ❍ Primary School Qualification
- ❍ Secondary School Qualification
- ❍ Tertiary Certificate
- ❍ Tertiary Diploma
- ❍ Some Undergraduate Degree Study
- ❍ Undergraduate Degree
- ❍ Postgraduate Degree
- ❍ Other (Please Specify) _____

Q4: Which geographical region do you currently live in?

- ❍ Northland
- ❍ Auckland
- ❍ Waikato
- ❍ Bay of Plenty
- ❍ Gisborne
- ❍ Hawkes Bay
- ❍ Taranaki
- ❍ Manawatu/Whanagui

- ❍ Wellington
- ❍ Nelson/Marlborough
- ❍ West Coast
- ❍ Canterbury
- ❍ Otago
- ❍ Southland
- ❍ Other (Please Specify) _____

Q5: Which of the following best describes the area that you currently live in?

- ❍ Urban area
- ❍ Rural area

Q6: Which of the following best describes your ethnic group? (Tick all that apply)

- ❑ New Zealand European
- ❑ Māori
- ❑ Samoan
- ❑ Cook Island Māori
- ❑ Tongan
- ❑ Niuean
- ❑ Chinese
- ❑ Indian
- ❑ other such as DUTCH, JAPANESE, TOKELAUAN. (Please Specify) _____
- ❑ Prefer not to say

Do you have any comments to add about the use of the Personalised Mobile Emergency Alert System (MEAS) before submitting the answers?

Appendix C. Measurement Items for Model

Construct & Definition	Measures (Items)
Perceived Severity (reflective) Estimates of the seriousness, or the severity of consequences of the event (Ifinedo, 2012).	• **[SEVR1]** If I were affected by an emergency situation like this: it would be severe. • **[SEVR2] …** it would be serious. • **[SEVR3]** … it would be problematic. • **[SEVR4]** If I were affected by an emergency like this, I would suffer a lot. • **[SEVR5]** Being affected by an emergency like this would be likely to cause me major problems. Questions repeated for Scenario #1 and Scenario #2
Perceived Vulnerability (reflective) An individual's assessment of the probability of threatening events (Ifinedo, 2012).	• **[VULN1]** My chances of being affected by an emergency situation like this in the future are high. • **[VULN2]** It is possible that I will be affected by an emergency situation like this. • **[VULN3]** I am at risk of being affected by an emergency situation like this in the future. • **[VULN4]** It is likely that I will be affected by an emergency situation like this. Questions repeated for Scenario #1 and Scenario #2
Fear (reflective) Fear refers to "a negatively valenced emotion representing a response that arises from recognizing danger. This response may include any combination of apprehension, fright, arousal, concern, worry, discomfort, or a general negative mood, and it manifests itself emotionally, cognitively, and physically." (Boss et al., 2015)	• **[FEAR1]** The prospect of being affected by an emergency situation like this would make me worried. • **[FEAR2]** … anxious. • **[FEAR3]** … scared. • **[FEAR4]** ... frightened. Questions repeated for Scenario #1 and Scenario #2

Maladaptive Reward (formative) Maladaptive rewards refer to any kind of rewards for the response of not protecting oneself from the threat (Boss et al., 2015).	• **[MALR1]** Not using a personalised MEAS would: ... save me time. • **[MALR2]** … save me money. • **[MALR3*]** … save me effort. • **[MALR4]** ... avoid false alarms. • **[MALR5]** … save me from taking unnecessary actions. • **[MALR6]** ... avoid unnecessary disruption. *Item was deleted
Response Efficacy (reflective) Response efficacy is the degree to which a person believes that the recommended response will be effective (Maddux and Rogers, 1983).	• **[REEF1]** Using a personalised MEAS would be a good way to reduce my risk of being affected by an emergency situation. • **[REEF2]** Using a personalised MEAS would lessen my chances of being affected by an emergency situation. • **[REEF3]** Using a personalised MEAS would be effective for protecting me from being affected by an emergency situation.
Self-Efficacy (reflective) Self-efficacy refers to "individual's ability or judgement regarding his or her capabilities to cope with or perform the recommended behaviour." (Ifinedo, 2012)	• **[SEEF1]** I feel confident in my ability to use a personalised MEAS. • **[SEEF2]** I have the resources to use a personalised MEAS. • **[SEEF3]** I have the knowledge necessary to use a personalised MEAS.
Response Cost (formative) Cost refers to any costs (e.g., monetary, personal, time, effort) associated with taking the adaptive coping response." (Floyed et al., 2000)	• **[COST1]** Mobile data for using a location-based service like a personalised MEAS would be costly. • **[COST2]** It would be time-consuming to set up a personalised MEAS (e.g. providing my personal data such as name, address, health information, etc.). • **[COST3]** It would be time-consuming to maintain my personal profile in a personalised MEAS (e.g. updating my mobile number, address, health information, etc.).

	• **[COST4]** Using a personalised MEAS may cause problems with other applications on my mobile devices. • **[COST5]** Using a personalised MEAS would require considerable investment of effort other than time. • **[COST6]** There are too many costs associated with using a location-based service like personalised MEAS.
Personalisation (reflective) Personalisation is defined as "the ability" to provide content and services based on knowledge about the individual (e.g. demographics, preferences, behavior, needs.)" (Adomavicius and Tuzhilin, 2005; Xu et al., 2011)	• **[PERS1]** A personalised MEAS could provide me with: ... emergency alert information that is tailored to my personal needs. • **[PERS2]** …the kind of emergency alert information that I might need. • **[RERS3]** ... emergency alert information that is specific to my situation.
Privacy Concern (reflective) Privacy concern refers to the "extent to which an individual is concerned" about organizational practices related to the collection and use of his or her personal information (Smith et al., 1996).	• **[MPRI1]** It would bother me if a personalised MEAS provider were to ask me for personal information. • **[MPRI2]** If a personalised MEAS provider asks me for personal information, I would think twice before providing it. • **[MPRI3]** I would be concerned that a MEAS provider would be collecting too much information about me.
Protection Motivation (reflective) In fear appeal research, protection motivation refers to one's intention to protect oneself from being harmed by the danger (Boss et al., 2015).	• **[INTE1]** If a personalised Mobile Emergency Alert Service (MEAS) were available to you: I intend to use a personalised MEAS. • **[INTE2]** … I plan to use a personalised MEAS. • **[INTE3]** … I predict I would use a personalised MEAS.

1. *The measures for the main model use 7-point Likert scale (End points were anchored by "Strongly Disagree" to "Strongly Agree")*